

Alcatel 5620

SERVICE AWARE MANAGER | RELEASE 2.0

USER GUIDE

Alcatel assumes no responsibility for the accuracy of the information presented, which is subject to change without notice.

Alcatel, the Alcatel logo, TiMetra, MainStreet, and Newbridge are registered trademarks of Alcatel. All other trademarks are the property of their respective owners.

Copyright 2004 Alcatel.
All rights reserved.

Disclaimers

Alcatel 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, licence or other distribution of the products for any such application without the prior written consent of Alcatel, shall be at the customer's sole risk. The customer hereby agrees to defend and hold Alcatel harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, licence or other distribution of the products in such applications.

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

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



PRINTED ON
RECYCLED PAPER

Alcatel License Agreement

SAMPLE END USER LICENSE AGREEMENT

1. LICENSE

- 1.1 Subject to the terms and conditions of this Agreement, Alcatel grants to Customer and Customer accepts a non-exclusive, non-transferable license to use any software and related documentation provided by Alcatel pursuant to this Agreement ("Licensed Program") for Customer's own internal use, solely in conjunction with hardware supplied or approved by Alcatel. In case of equipment failure, Customer may use the Licensed Program on a back-up system, but only for such limited time as is required to rectify the failure.
- 1.2 Customer acknowledges that Alcatel may have encoded within the Licensed Program optional functionality and capacity (including, but not limited to, the number of equivalent nodes, delegate work stations, 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 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 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, 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 may terminate this Agreement: (a) upon notice to Customer if any amount payable to Alcatel 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.

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 non-use, shall survive termination.

4. CHARGES

4.1 Upon shipment of the Licensed Program, Alcatel 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 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 to Customer from time to time.

6. WARRANTIES AND INDEMNIFICATION

6.1 Alcatel 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's sole liability and Customer's sole remedy for a breach of this warranty shall be Alcatel's good faith efforts to rectify the nonconformity or, if after repeated efforts Alcatel is unable to rectify the non-conformity, Alcatel 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 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 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 infringes any patent, copyright, trade secret or other intellectual property right, provided that Customer notifies Alcatel within ten (10) days of the existence of the claim, gives Alcatel sole control of the litigation or settlement of the claim, and provides all such assistance as Alcatel may reasonably require. Notwithstanding the foregoing, Alcatel 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 against any such claim.
- 6.4 Alcatel 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, licence or other distribution of the Products for any such application without the prior written consent of Alcatel, shall be at the Customer's sole risk. The Customer also agrees to defend and hold Alcatel harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, licence 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, 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, ITS EMPLOYEES, DIRECTORS, OFFICERS OR AGENTS FOR ALL CLAIMS EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER TO ALCATEL 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'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 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 from a third party source. No license fee has been paid by Alcatel 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 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, re-export, 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

About this document

The *Alcatel 5620 SAM User Guide* provides task-based workflows and user documentation to allow you to:

- use the GUI to perform tasks and maximize operator efficiency
- auto-discover and administer the 5620 SAM-managed network
- configure 7750 SR and 7450 ESS equipment
- set and enable QoS and routing policies
- set and configure customer services, such as VLL, IES, VPRN, and VPLS
- manage network faults
- collect accounting and performance statistics

The *Alcatel 5620 SAM User Guide* uses a task-based format. Each chapter contains:

- overview information about the task or function
- a workflow describing the steps necessary to complete the task or execute the functionality
- menus or commands used to complete the procedure
- a list of required procedures
- detailed procedures with key parameter descriptions and GUI windows that display the configuration options

About related documentation

There are many documents that define the 5620 SAM and the managed devices.

- Use the *Alcatel 5620 SAM Installation Guide* to install the database, server, and client 5620 SAM software.
- Use the *Alcatel 5620 SAM-O OSS Interface Developer Guide* to use the XML OSS interface to create OSS applications, such as alarm monitoring and inventory controls.
- Use the *Alcatel 5620 SAM Network Management Troubleshooting Guide* to troubleshoot 5620 SAM applications and platforms
- See the index file in the User Documentation directory on the application CD-ROM for additional documentation.

See the 7750 SR and 7450 ESS user documentation guides for more detailed information about specific CLI commands, device installation, and additional parameter information.

Conventions used in this guide

The following table lists the conventions that are used throughout the documentation.

Table 1 Documentation conventions

Convention	Description	Example
Key name	Press a keyboard key	Delete
Italics	Identifies a variable	<i>hostname</i>
Key+Key	Type the appropriate consecutive keystroke sequence	CTRL+G
Key–Key	Type the appropriate simultaneous keystroke sequence	CTRL–G
↵	Press the Return key	↵
—	An em dash indicates there is no information.	—
→	Indicates that a cascading submenu results from selecting a menu item	Policies→Alarm Policies

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.

Important information

The following conventions are used to indicate important information:



Note — A note provides information that is, or may be, of special interest.



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



Warning — A warning indicates that the described activity or situation may, or will, cause equipment damage.

Contents

Preface	ix
About this document.....	ix
About related documentation.....	x
Conventions used in this guide.....	x
Procedures with options or substeps	x
Important information	xi

Getting started

1 — Workflows	1-1
1.1 5620 SAM workflow	1-2
1.2 Workflow to install, configure, create, and manage end-user services.....	1-2
2 — Before you start	2-1
2.1 5620 SAM overview	2-2
2.2 Changing 5620 SAM configurations	2-2
2.3 Enabling functionality before using the 5620 SAM	2-3
Procedure 2-1 To enable functionality before using the 5620 SAM.....	2-3
2.4 New for this release of the 5620 SAM	2-4
2.5 Basic FAQs to troubleshoot the 5620 SAM	2-8
How do I limit the number of reads and writes to the router?	2-8
How should I name objects on the GUI?	2-8

3 —	The GUI	3-1
3.1	GUI overview	3-2
3.2	GUI workflow	3-3
3.3	GUI menus.....	3-3
3.4	GUI procedures	3-4
3.5	GUI basic operation procedures	3-4
	Procedure 3-1 To start the 5620 SAM GUI from a PC.....	3-4
	Procedure 3-2 To start the 5620 SAM GUI from a Solaris workstation	3-5
	Procedure 3-3 To disable or enable the GUI activity check.....	3-5
	Procedure 3-4 To use menus, the toolbar, or shortcuts.....	3-5
	Procedure 3-5 To navigate the GUI	3-6
	Procedure 3-6 To use windows, drawings, and forms to set or view parameters.....	3-6
	Procedure 3-7 To view and manipulate listed information	3-9
	Procedure 3-8 To save list preferences.....	3-10
	Procedure 3-9 To view software release and license key information.....	3-10
	Procedure 3-10 To exit the 5620 SAM GUI	3-11
4 —	Form management	4-1
4.1	Forms overview	4-2
4.2	Forms management workflow.....	4-3
4.3	Forms management procedures list	4-3
4.4	Window menu options	4-4
4.5	Form management procedures	4-4
	Procedure 4-1 To arrange forms in the working pane	4-4
	Procedure 4-2 To bring an open form to the foreground	4-5
	Procedure 4-3 To close forms.....	4-5
5 —	Search and find functions	5-1
5.1	Performing searches overview	5-2
5.2	Performing searches workflow.....	5-2
5.3	Performing searches menu.....	5-2
5.4	Performing searches procedures list	5-3
5.5	Performing searches procedures.....	5-3
	Procedure 5-1 To perform a simple search from the Find menu	5-3
	Procedure 5-2 To perform a search using the Search button.....	5-5
	Procedure 5-3 To perform a search using the Select button	5-6

Discovering routers and administering the network

6 —	Discovery manager	6-1
6.1	Network element discovery overview	6-2
6.2	Discovery workflow	6-3
6.3	Discovery menus	6-3

6.4	Discovery procedures list.....	6-3
6.5	Discovery procedures	6-4
	Procedure 6-1 To configure poller policies	6-4
	Procedure 6-2 To configure polling policies and discovery to use SNMPv3.....	6-8
	Procedure 6-3 To discover devices	6-9
	Procedure 6-4 To edit a discovery rule	6-14
	Procedure 6-5 To enable or disable a discovery rule	6-15
	Procedure 6-6 To remove a discovery rule.....	6-16
	Procedure 6-7 To rescan the network.....	6-16
	Procedure 6-8 To manage or unmanage a device	6-16
	Procedure 6-9 To reconcile device elements in the 5620 SAM database	6-17
6.6	SNMP MIBs	6-18
7 —	In-band and out-of-band management	7-1
7.1	Network element in-band and out-of-band management overview	7-2
7.2	In-band and out-of-band management workflow	7-3
7.3	In-band and out-of-band management menu	7-4
7.4	In-band and out-of-band management procedure list.....	7-4
7.5	In-band and out-of-band management procedure	7-4
	Procedure 7-1 To configure in-band or out-of-band polling policies	7-4
8 —	Security management for 5620 SAM groups and users	8-1
8.1	Security management for 5620 SAM groups and users overview	8-2
	Users and group permissions	8-3
8.2	Workflow to manage security for 5620 SAM groups and users.....	8-4
8.3	5620 SAM groups and users configuration procedures list	8-4
8.4	5620 SAM groups and user configuration procedures	8-5
	Procedure 8-1 To create 5620 SAM user groups	8-5
	Procedure 8-2 To create 5620 SAM user accounts.....	8-6
	Procedure 8-3 To delete 5620 SAM groups	8-7
	Procedure 8-4 To delete 5620 SAM user accounts.....	8-8
	Procedure 8-5 To suspend or re-instate 5620 SAM users.....	8-8
	Procedure 8-6 To change 5620 SAM user passwords as system administrator	8-9
	Procedure 8-7 To change a 5620 SAM user password as user	8-9
9 —	Security management for 7750 SR users with RADIUS or TACACS+	9-1
9.1	Security management for 7750 SR using RADIUS AND TACACS+ overview.....	9-2
	7750 SR users and group permissions.....	9-3
	RADIUS and TACACS+ policies and permissions	9-3
9.2	Workflow to manage security for 7750 SR users and RADIUS or TACACS+	9-3
9.3	7750 SR user and RADIUS or TACACS+ menus.....	9-4
9.4	7750 SR user and RADIUS or TACACS+ configuration procedures list	9-4
9.5	Device security configuration procedures.....	9-5

	Procedure 9-1 To create or modify site management access filter policies for managed devices.....	9-5
	Procedure 9-2 To create user profiles for managed device access.....	9-8
	Procedure 9-3 To create, modify, and manage user accounts for access to managed devices.....	9-9
	Procedure 9-4 To specify or modify password policies.....	9-12
	Procedure 9-5 To create RADIUS access policies	9-13
	Procedure 9-6 To create TACACS+ access policies	9-14
	Procedure 9-7 To distribute policies	9-16
10 —	Deployment and site backup/upgrade management	10-1
10.1	Deployment and site backup/upgrade overview	10-2
10.2	Workflow for deployment and site backup/upgrade.....	10-2
10.3	Deployment and site backup/upgrade menu	10-2
10.4	Deployment and site backup/upgrade procedures list.....	10-3
10.5	Deployment and site backup/upgrade procedures	10-3
	Procedure 10-1 To configure a 5620 SAM-to-node deployment policy	10-3
	Procedure 10-2 To troubleshoot a configuration deployment.....	10-5
	Procedure 10-3 To schedule a device backup.....	10-5
	Procedure 10-4 To start an immediate backup or restore	10-7
	Procedure 10-5 To upgrade the node software image	10-8
	Procedure 10-6 To view the status of the backup, restore, or upgrade	10-9
11 —	5620 SAM database manager	11-1
11.1	5620 SAM database manager overview	11-2
11.2	Workflow to manage the 5620 SAM database	11-2
11.3	5620 SAM database menu	11-2
11.4	5620 SAM database procedures list.....	11-2
11.5	5620 SAM database procedures	11-3
	Procedure 11-1 To view general database statistics	11-3
	Procedure 11-2 To analyze the database.....	11-4
	Procedure 11-3 To back up the database.....	11-6
12 —	Using CLI from the 5620 SAM	12-1
12.1	CLI overview	12-2
12.2	Workflow to use the CLI.....	12-2
12.3	CLI menus	12-2
12.4	CLI procedure list.....	12-3
12.5	CLI procedures	12-3
	Procedure 12-1 To launch a CLI session.....	12-3
	Procedure 12-2 To configure CLI console terminal preferences	12-4
	Procedure 12-3 To create and use CLI scripts	12-5
	Procedure 12-4 To save CLI scripts	12-7

Router and IP/MPLS network configuration and

management

13 —	Equipment management overview	13-1
13.1	Equipment management overview	13-2
13.2	Working with objects	13-3
	Procedure 13-1 To create an object	13-4
13.3	Working with network objects	13-4
13.4	Working with device objects	13-5
	7750 SR support	13-5
	7450 ESS support	13-6
13.5	Working with LAG objects	13-7
13.6	Working with shelf objects	13-8
13.7	Working with card and card slot objects	13-8
13.8	Working with daughter card objects	13-9
13.9	Working with port and channel objects	13-10
	Connection termination points for services and interfaces	13-11
	STS3 to STS192 clear channel	13-11
	DS3 clear channel	13-12
	DS0 channel groups	13-12
	Ethernet ports	13-12
	SONET STS1 channelization and SONET clear-channel applications	13-13
	TDM channelization and clear channel applications	13-15
14 —	Equipment management using the navigation tree	14-1
14.1	Navigation tree overview	14-2
	Contextual menus for objects in the navigation tree	14-3
14.2	Workflow to manage equipment using the navigation tree	14-7
14.3	Navigation tree menus	14-7
14.4	Navigation tree procedures list	14-7
14.5	Navigation tree procedures	14-8
	Procedure 14-1 To group devices and routers	14-8
	Procedure 14-2 To change device properties	14-10
	Procedure 14-3 To create and configure a LAG	14-10
	Procedure 14-4 To create a card type	14-13
	Procedure 14-5 To create daughter cards	14-13
	Procedure 14-6 To configure Ethernet ports	14-14
	Procedure 14-7 To configure SONET ports	14-18
	Procedure 14-8 To configure TDM ports	14-23
	Procedure 14-9 To configure SONET clear channels and SONET STS1 sub-channels	14-24
	Procedure 14-10 To configure TDM channels	14-26
15 —	Equipment management using the equipment manager	15-1
15.1	Equipment manager overview	15-2
	Equipment manager forms	15-2
15.2	Workflow to manage equipment using the Equipment manager	15-7
15.3	Equipment manager menu	15-8
15.4	Equipment manager procedures list	15-8

15.5	Equipment manager procedures	15-8
	Procedure 15-1 To use the network element filter	15-8
	Procedure 15-2 To change the configuration of devices using the equipment manager	15-9
16	— Router configuration	16-1
16.1	Router configuration overview	16-2
16.2	Workflow to configure routers	16-3
16.3	Router configuration menus	16-4
16.4	Router configuration procedures list	16-5
16.5	Router configuration procedures	16-5
	Procedure 16-1 To configure router routing instance parameters	16-5
	Procedure 16-2 To configure or modify a Layer 3 interface	16-7
	Procedure 16-3 To configure a routing policy	16-11
	Procedure 16-4 To configure an MPLS administrative group policy	16-16
	Procedure 16-5 To configure a static route	16-18
17	— Routing protocol configuration	17-1
17.1	Routing protocol configuration overview	17-2
	BGP	17-3
	RIP	17-5
	OSPF	17-5
	LDP	17-7
	ISIS	17-8
17.2	Workflow to configure routing protocols	17-10
17.3	Routing protocol configuration menus	17-11
17.4	Routing protocol configuration procedures list	17-11
17.5	Routing protocol configuration procedures	17-12
	BGP	17-12
	Procedure 17-1 To enable BGP on a router	17-13
	Procedure 17-2 To configure global-level BGP	17-14
	Procedure 17-3 To configure a BGP confederation	17-16
	Procedure 17-4 To configure peer group-level BGP	17-19
	Procedure 17-5 To configure peer-level BGP	17-19
	RIP	17-20
	Procedure 17-6 To configure global-level RIP	17-20
	Procedure 17-7 To configure group-level RIP	17-21
	Procedure 17-8 To configure interface-level RIP	17-22
	OSPF	17-22
	Procedure 17-9 To enable OSPF on a router	17-23
	Procedure 17-10 To configure OSPF on a router	17-24
	Procedure 17-11 To configure an OSPF area and add Layer 3 interfaces to the area	17-25
	Procedure 17-12 To add a router to an OSPF area	17-28
	Procedure 17-13 To create a virtual link	17-30
	LDP	17-30
	Procedure 17-14 To enable LDP on a router	17-30
	Procedure 17-15 To configure global-level LDP parameters	17-31
	Procedure 17-16 To configure LDP interfaces	17-33
	Procedure 17-17 To configure LDP targeted peers	17-34

ISIS	17-36
Procedure 17-18 To enable ISIS	17-36
Procedure 17-19 To configure ISIS parameters	17-37
Procedure 17-20 Configure ISIS NET addresses	17-39
Procedure 17-21 To configure ISIS interfaces	17-40

18 — MPLS 18-1

18.1	MPLS configuration overview	18-2
18.2	Workflow to configure MPLS	18-4
18.3	MPLS menus	18-4
18.4	MPLS procedures list	18-4
18.5	MPLS procedures	18-5
	Procedure 18-1 To enable MPLS on a routing instance	18-5
	Procedure 18-2 To create MPLS interfaces	18-5
	Procedure 18-3 To create MPLS paths	18-7
	Procedure 18-4 To create LSPs	18-9
	Procedure 18-5 To configure LSP paths	18-14
	Procedure 18-6 To list MPLS paths	18-15
	Procedure 18-7 To list LSPs	18-16
	Procedure 18-8 To view the LSP topology map	18-16

19 — Service tunnels 19-1

19.1	Service tunnel overview	19-2
19.2	Service tunnel menus	19-3
19.3	Service tunnel procedure list	19-3
19.4	Configuring service tunnels procedures	19-4
	Procedure 19-1 To configure service tunnels	19-4
	Procedure 19-2 To list service tunnels	19-6
	Procedure 19-3 To view the service tunnel topology map	19-6

Managing subscriber services

20 — Policies 20-1

20.1	Policies overview	20-2
20.2	Service management policies	20-5
	Access ingress policies	20-5
	Access egress policies	20-8
	Network policies	20-9
	Network Queue policies	20-10
	Slope policies	20-11
	Scheduler policies	20-13
	Filter policies	20-15
20.3	Workflow to create policies	20-17
20.4	Policies menu	20-17
20.5	Policies procedures list	20-18
20.6	Policies procedures	20-19

	Procedure 20-1 To create an access ingress policy	20-19
	Procedure 20-2 To create an access egress policy	20-22
	Procedure 20-3 To create a network policy	20-24
	Procedure 20-4 To create a slope policy	20-25
	Procedure 20-5 To create a network queue policy	20-27
	Procedure 20-6 To create a scheduler policy	20-32
	Procedure 20-7 To create an aggregation scheduler	20-34
	Procedure 20-8 To create an Acl IP filter policy	20-35
	Procedure 20-9 To create an Acl MAC filter policy	20-36
	Procedure 20-10 To distribute a policy	20-38
	Procedure 20-11 To edit a policy	20-39
	Procedure 20-12 To delete a policy	20-39
	Procedure 20-13 To copy or overwrite a policy	20-40
	Procedure 20-14 To synchronize a policy	20-40
	Procedure 20-15 To remove an unassociated policy	20-41
21 —	Subscriber configuration and management	21-1
21.1	Subscriber overview	21-2
21.2	Workflow to configure and manage subscribers	21-2
21.3	Subscriber menu	21-3
21.4	Subscriber configuration and management procedures list	21-3
21.5	Subscriber configuration and management procedures	21-3
	Procedure 21-1 To create subscribers	21-4
	Procedure 21-2 To modify and manage subscriber information	21-5
	Procedure 21-3 To delete subscribers	21-7
	Procedure 21-4 To view subscriber maps	21-7
22 —	Service management overview	22-1
22.1	Service management overview	22-2
22.2	Access interfaces	22-6
22.3	Sample network configuration using HQoS	22-7
23 —	VLL service management	23-1
23.1	VLL service management overview	23-2
23.2	Sample VLL service	23-4
23.3	Workflow to create a VLL service	23-6
23.4	VLL service management menus	23-6
23.5	VLL service management procedures list	23-7
23.6	VLL service management procedures	23-7
	Procedure 23-1 To create a VLL service	23-7
	Procedure 23-2 To modify a VLL service	23-20
	Procedure 23-3 To add access spoke circuits for an HVPLS	23-21
	Procedure 23-4 To delete a VLL service	23-21
	Procedure 23-5 To view the service topology	23-21
24 —	VPLS management	24-1
24.1	VPLS management overview	24-2
	HVPLS	24-4

	FIBs.....	24-5
	MAC learning	24-6
	Flooding	24-6
	Spanning tree protocols	24-6
24.2	Sample VPLS configuration	24-7
24.3	Workflow to create a VPLS	24-13
24.4	VPLS management menus	24-14
24.5	VPLS management procedures list	24-14
24.6	VPLS management procedures	24-14
	Procedure 24-1 To create a VPLS	24-15
	Procedure 24-2 To modify a VPLS	24-33
	Procedure 24-3 To delete a VPLS	24-34
	Procedure 24-4 To configure HVPLS using access spoke circuits.....	24-35
	Procedure 24-5 To add or modify FIB entries	24-38
	Procedure 24-6 To view the service topology	24-40
25	— IES management	25-1
25.1	IES management overview	25-2
25.2	Sample IES configuration	25-3
25.3	Workflow to create an IES	25-5
25.4	IES management menus	25-5
25.5	IES management procedures list.....	25-5
25.6	IES management procedures	25-6
	Procedure 25-1 To create an IES	25-6
	Procedure 25-2 To modify an IES.....	25-21
	Procedure 25-3 To delete an IES	25-21
	Procedure 25-4 To view the service topology	25-22
26	— VPRN service management	26-1
26.1	VPRN service management overview	26-2
	VPRN service routers	26-3
	Policies.....	26-4
	Troubleshooting	26-4
26.2	Sample VPRN configuration	26-4
26.3	Workflow to create a VPRN service.....	26-6
26.4	VPRN service management menus.....	26-7
26.5	VPRN service management procedures list	26-7
26.6	VPRN service management procedures	26-8
	Procedure 26-1 To create a VPRN service.....	26-8
	Procedure 26-2 To modify a VPRN	26-33
	Procedure 26-3 To delete a VPRN	26-33
	Procedure 26-4 To view the service topology	26-34
27	— Map management	27-1
27.1	Network topology maps overview	27-2
	LSP topology map.....	27-2
	LSP path topology map.....	27-3
	Service topology map	27-4
	Service path topology maps.....	27-6

27.2	Map management workflow	27-7
27.3	Map menus	27-7
27.4	Map management procedures list	27-7
27.5	Map management procedures	27-8
	Procedure 27-1 To open a map	27-8
	Procedure 27-2 To view and understand map elements	27-8
	Procedure 27-3 To open the LSP path map from the MPLS Path Manager	27-9
	Procedure 27-4 To open the LSP path map from the LSP Path Manager	27-9
	Procedure 27-5 To list or view object information from a map.....	27-10
	Procedure 27-6 To zoom in and zoom out of a map.....	27-10

Fault management

28 — Fault management using alarms 28-1

28.1	Fault management using alarms overview	28-2
28.2	Workflow to manage network faults using alarms	28-4
28.3	Fault management alarms menus	28-5
28.4	Fault management using alarms procedures list	28-5
28.5	Fault management using alarms procedures	28-6
	Procedure 28-1 To set global alarm policies.....	28-6
	Procedure 28-2 To set alarm history behavior.....	28-8
	Procedure 28-3 To set specific alarm policies	28-10
	Procedure 28-4 To view alarms raised against equipment, logical components, and services	28-11
	Procedure 28-5 To view alarm information.....	28-12
	Procedure 28-6 To view all network alarms using the dynamic alarm list.....	28-17
	Procedure 28-7 To view network alarm statistics	28-19
	Procedure 28-8 To review historical alarms.....	28-19
28.6	Alarm descriptions	28-20

29 — Troubleshooting and fault management using OAM 29-1

29.1	Troubleshooting and fault management using OAM overview	29-2
	MTU ping OAM	29-3
	Tunnel ping OAM.....	29-3
	Circuit ping OAM.....	29-4
	LSP ping OAM	29-4
	LSP trace OAM.....	29-4
	MAC ping OAM.....	29-5
	MAC trace OAM.....	29-6
	MAC populate OAM	29-6
	MAC purge OAM.....	29-6
	VPRN ping and VPRN trace	29-7
29.2	Workflow to manage network faults using OAM tools	29-7
29.3	Fault management OAM menus.....	29-8

29.4	Fault management using OAM diagnostics procedures list.....	29-8
29.5	Fault management using OAM diagnostics procedures	29-9
	Procedure 29-1 To perform OAM diagnostics from a service tunnel	29-9
	Procedure 29-2 To perform OAM diagnostics from a service	29-13
	Procedure 29-3 To interpret OAM diagnostic results	29-22

Performance monitoring using statistics

30 — Accounting and performance monitoring using statistics

		30-1
30.1	Accounting and performance monitoring using statistics overview	30-2
	Accounting	30-2
	Performance monitoring.....	30-3
	Statistical policies, values, and counters	30-4
30.2	Workflow for statistics collection	30-18
30.3	Statistics menus.....	30-19
30.4	Statistics procedure list.....	30-19
30.5	Performance monitoring using statistics procedures	30-20
	Procedure 30-1 To create or modify a file policy	30-20
	Procedure 30-2 To create or modify an accounting policy.....	30-22
	Procedure 30-3 To view equipment and other object-based performance statistics	30-25
	Procedure 30-4 To modify equipment and object-based performance statistics policies	30-26
	Procedure 30-5 To view statistics logs	30-28

Glossary

Index

Getting started

- 1 — Workflows**
- 2 — Before you start**
- 3 — The GUI**
- 4 — Form management**
- 5 — Search and find functions**

1 — Workflows

1.1 5620 SAM workflow 1-2

1.2 Workflow to install, configure, create, and manage end-user services 1-2

1.1 5620 SAM workflow

The 5620 SAM workflow describes how to use the client GUI software.

Use this workflow to:

- install, configure, create, and manage end-user services
- determine which workflow functions meet your user needs, then perform those functions

1.2 Workflow to install, configure, create, and manage end-user services

This workflow combines all workflows created for the 5620 SAM.

- 1 Install the 5620 SAM software, as described in the *Alcatel 5620 SAM Installation Guide*.
- 2 Start using the GUI.
 - a Enable device functionality and optionally review the new features; see chapter 2.
 - b Start the GUI and become familiar with GUI basics to navigate and use the 5620 SAM functions; see chapter 3.
 - c Manage GUI windows and forms; see chapter 4.
 - d Use the find and filter functions of the GUI to search quickly for equipment, network objects, or services; see chapter 5.
- 3 Perform system administration tasks for the 5620 SAM system.
 - a Discover the managed network and start managing equipment and services; see chapter 6.
 - b If required, modify polling to use in-band or out-of-band management; see chapter 7.
 - c Create a secure network management system and enable 5620 SAM users and accounts; see chapter 8.
 - d Create security policies on the managed devices and create accounts for users to securely access the managed devices using management access filters, RADIUS, or TACACS+ authentication; see chapter 9.
 - e Perform managed device database management tasks, for example, backing up a 7750 SR database; see chapter 10.
 - f Perform 5620 SAM database tasks, for example backing up the 5620 SAM database; see chapter 11.
 - g Use the CLI telnet or SSH consoles from the 5620 SAM to view and configure managed devices, and to create CLI scripts; see chapter 12.

- 4 Review how physical equipment is configured and managed; see chapter 13.
 - a Configure and manage physical equipment using the navigation tree; see chapter 14.
 - b Configure and manage physical equipment using the Equipment Manager; see chapter 15.
- 5 Configure the device to set up network protocol communications and connections, such as MPLS LSPs, to allow customer traffic to flow from the access network through the core network.
 - a Configure the device and router interfaces; see chapter 16.
 - b Configure routing protocols; see chapter 17.
 - c Configure MPLS and LSPs; see chapter 18.
 - d Configure service tunnels (also known as SDPs); see chapter 19.
- 6 Determine and configure subscriber-based policies, such as QoS, and services, such as VLL, that can be configured to provide services to customers.
 - a Determine and configure local or global policies, such as QoS and filtering, that specify the quality of services delivered; see chapter 20.
 - b Become familiar with service concepts, such as access interfaces and associating subscribers with services; see chapter 22.
 - c Configure and manage your subscriber (customer) base; see chapter 21.
 - d Configure VLL services for subscribers, which provides point-to-point connectivity between customer-facing access ports; see chapter 23.
 - e Configure VPLS services for subscribers, which provides a virtual LAN so multiple customer sites can be connected in a single bridged domain contained within the same IP/MPLS network; see chapter 24.
 - f Configure IES services for subscribers, which provides an IP router interface for customers to send and receive Internet traffic; see chapter 25.
 - g Configure VPRN services for subscribers, which provides a virtual IP LAN to connect multiple customer sites using L3 interfaces; see chapter 26.
 - h View the topology of both the services subscribed to by customers and the service path topology used to route traffic by looking at maps; see chapter 27.
- 7 Monitor and troubleshoot customer services and the physical and logical network for faults.
 - a Use alarm to correlate network faults with impacts to subscriber services, and configure alarm policies; see chapter 28.
 - b Use OAM tools, such as MTU OAM and MAC trace, to troubleshoot circuits, service tunnels, and subscriber traffic down to the individual service level; see chapter 29.
- 8 Track network performance, equipment usage, billing data, and SLAs using accounting and performance statistics counters; see chapter 30.

2 — Before you start

- 2.1 5620 SAM overview 2-2**
- 2.2 Changing 5620 SAM configurations 2-2**
- 2.3 Enabling functionality before using the 5620 SAM 2-3**
- 2.4 New for this release of the 5620 SAM 2-4**
- 2.5 Basic FAQs to troubleshoot the 5620 SAM 2-8**

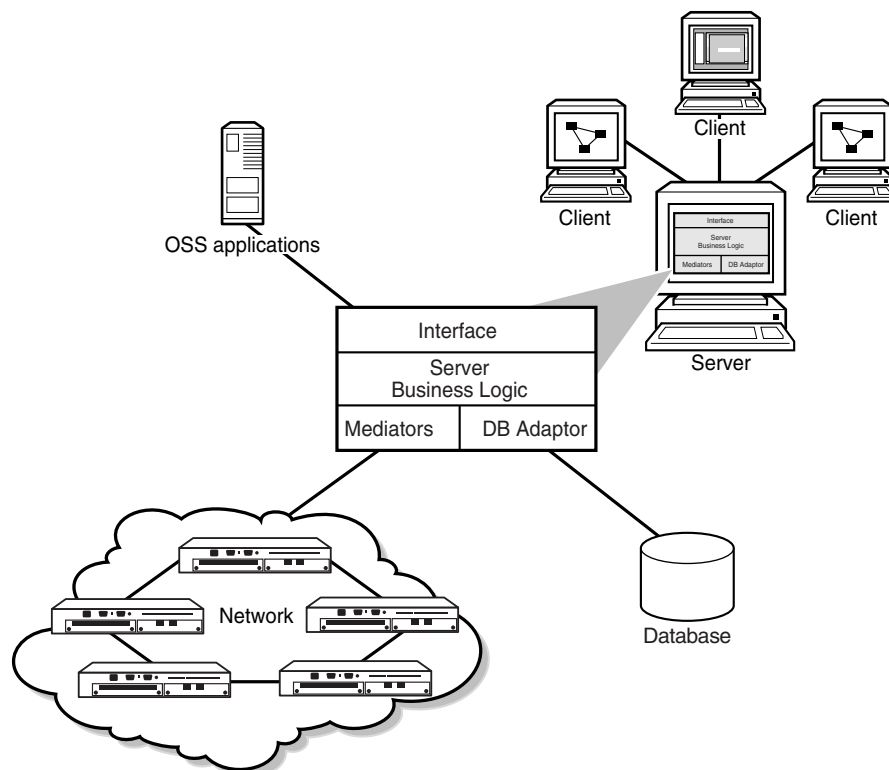
2.1 5620 SAM overview

The 5620 SAM is a network management system that is used to manage devices, such as the 7750 SR, by simplifying network management tasks.

The distributed 5620 SAM elements, collectively known as the 5620 SAM portfolio, run on independent networkstations. These databases, servers, and clients were created when the 5620 SAM database, server, and client software was installed. The installation is described in the *Alcatel 5620 SAM Installation Guide*.

The GUI and network management components use a Java-based technology that provides distributed, secure, and scalable applications. This architecture allows for scaling and fair load balancing, which improves performance. GUIs run on clients, and do not have direct access to the database or the network elements. Figure 2-1 shows the basic architecture.

Figure 2-1 5620 SAM architecture



17189

2.2 Changing 5620 SAM configurations

You can change the configuration of the 5620 SAM database, server, and client networkstations using the 5620 SAM installation software, as described in the *Alcatel 5620 SAM Installation Guide*.

Change the configuration when:

- Network Operations Centre topology changes
- new PCs or networkstations are brought online as a database, server, or clients

2.3 Enabling functionality before using the 5620 SAM

Complete the following procedure on each managed router before you use the 5620 SAM.

Procedure 2-1 To enable functionality before using the 5620 SAM

See the appropriate router documentation for more information about using the CLI.

- 1 Enable the system ID of the 7750 SRs to be managed by the 5620 SAM:

- i Run the following CLI command on the 7750 SRs, in sequence:

```
configure router interface system
```

```
address <a.b.c.d>/32
```

where <a.b.c.d> is the system ID and /32 is the bitmask

- ii Close CLI.

- 2 Run the following CLI command to enable the SNMP engine and configure at least one SNMPv2 community on all 7750 SRs to be managed by the 5620 SAM:

```
configure system snmp no shutdown
```

```
configure system security snmp community name of community rwa  
version both
```

where *name of community* is the SNMPv2 community name

```
admin save
```

- 3 Run the following CLI command on all 7750 SRs to be managed by the 5620 SAM to ensure that all get SNMP PDU commands are properly run:

```
system snmp packet-size 9216
```

```
admin save
```

- 4 Run the following CLI command to ensure persistent SNMP indexes are used:

```
bof
persist on
save
back
admin save
admin synchronize boot-env
admin reboot
Are you sure you want to reboot? (y/n) y
```

If the router was already managed, unmanage (delete) the router and rediscover the router.

- 5 Now that SNMP communication is enabled, ensure that SNMP trap configuration is running using the following CLI command:

```
configure log
info
```

Check the output for the following information.

- an SNMP trap group
 - that the SNMP trap group is associated with the IP address of the 5620 SAM server
-

2.4 New for this release of the 5620 SAM

Table 2-1 lists the new features or functionality in this release of the 5620 SAM.

Table 2-1 New 5620 SAM functionality

Feature or function	How and why to use it	Reference for more information
VPRN service	<p>The 5620 SAM supports the creation of VPRN services using the 7750 SR as a PE and provider core (P) router. VPRNs, which are also called IP VPNs or BGP/MPLS VPNs, are defined in RFC 2547bis, which details a method of forwarding data and distributing routing information across an IP/MPLS provider core network.</p> <p>A VPRN service consists of CE devices connected to PE routers. PE routers connected to P routers transport data across the IP/MPLS provider core network in service tunnels. The 5620 SAM supports the creation of GRE or MPLS LSP service tunnels.</p>	See chapter 26 for overview and configuration information.
Router security management, including user domain control and using TACACS+ or RADIUS authentication	<p>Security support for accessing the managed routers, such as the 7750 SR, in the following ways:</p> <ul style="list-style-type: none"> • Create and manage users, management access filters, profiles, and passwords for access to the managed routers. • Configure RADIUS or TACACS+ authentication to allow controlled access to the managed routers using 5620 SAM user accounts. <p>RADIUS and TACACS+ are access server AAA protocols. Each protocol provides a standardized method of exchanging information between a RADIUS or TACACS+ client, located on the managed router, and a RADIUS or TACACS+ server, located externally from the managed router and the 5620 SAM.</p>	See chapter 9 for overview and configuration information.
LSP, VPRN, and MAC OAM diagnostics	<p>The LSP ping and traceroute diagnostics provide a mechanism to detect data plane failures in MPLS LSPs. The diagnostics are modeled after the ICMP echo request/reply used to detect and isolate faults in IP networks.</p> <p>The following MAC OAM diagnostics are supported.</p> <ul style="list-style-type: none"> • MAC ping determines whether an egress service access point that binds a given MAC address within a VPLS service exists. • MAC trace OAM displays the hop-by-hop route of MAC addresses used to reach the target MAC address at the far end. • MAC populate OAM populates a service FIB with an OAM-tagged MAC entry. 	See chapter 29 for overview and configuration information.
Support for new hardware	<p>7450 ESS chassis configurations that are managed include the following shelf types:</p> <ul style="list-style-type: none"> • 1-slot with 1 I/O slot that supports 2 daughter cards • 7-slots with 6 slots that support 12 daughter cards. <p>Additional card and port support, including:</p> <ul style="list-style-type: none"> • 12-port DS3 to the T1/E1 and DS0 level and E3 to the E3 level on the 7750 SR • 1-port OC12/STM4 to the DS0 level on the 7750 SR • Gigabit Ethernet with 10- and 20-ports on the 7450 ESS • 10XGigabit Ethernet with 1 port LAN/WAN physical card on the 7450 ESS 	<p>See the appropriate hardware documentation for card and port information, such as line length and hardware specifications.</p> <p>See chapter 13 for information about hardware modelling support by the 5620 SAM.</p> <p>See Table 13-3 for a list of supported cards and ports on the managed hardware.</p>

(1 of 4)

Feature or function	How and why to use it	Reference for more information
XML northbound OSS interfaces	<p>An OSS application uses the Alcatel 5620 SAM Open Interfaces XML interface to configure or access network management information contained in the 5620 SAM database. The XML interface can then receive information from or manipulate the managed object model. All transactions with the 5620 SAM database are processed by the 5620 SAM server.</p> <p>The 5620 SAM-O XML interface allows OSSs to:</p> <ul style="list-style-type: none"> • access all 5620 SAM FCAPS functionality for read, or read and write methods • ensure backward compatibility • access functionality using HTTP or HTTPS and simple SOAP encoding • securely transport requests and receive responses 	See the <i>Alcatel 5620 SAM-O OSS Interface Developer Guide</i> .
ISIS protocol support	<p>ISIS is a link-state interior gateway protocol that uses the shortest path first algorithm to make routing decisions. ISIS entities consist of:</p> <ul style="list-style-type: none"> • networks, which are autonomous system routing domains • intermediate systems, which are routers such as the 7750 SRs • end systems, which are network devices that send and receive PDUs <p>The ISIS information displayed and configured from the GUI includes:</p> <ul style="list-style-type: none"> • a backbone area and the devices in the backbone area • a list of areas with the devices that are participating in the area • the open the area devices to display the interface IP addresses with the configured level (1, 2, or 1 and 2) of each interface 	See the ISIS overview, configuration, and procedural information in chapter 17.
Protocol support enhancements for BGP and LDP	<p>From the GUI, you can enable and configure LDP parameters. From the network tab routing instance, there are two trees for LDP: Interfaces and Targeted LDP Peers.</p> <p>LDP is used to distribute labels. devices can establish LSPs across a network by mapping network-layer routing information directly to the data link layer-switched paths. After LDP distributes the labels to the LSRs, the LSR assigns the label to a FEC, and then informs all other LSRs in the path know about the label and how the label will switch data accordingly.</p> <p>T-LDP is supported on 7750 SRs and 7450 ESSs, DU-LDP is only supported on the 7750 SR.</p> <p>You can use the 5620 SAM to enable BGP on the device and to:</p> <ul style="list-style-type: none"> • set the AS values for the routing instance • create confederations to group-managed routers • create BGP peer groups • create neighbors within the BGP peer groups 	See the BGP and LDP overview, workflow, and procedures in chapter 17.

(2 of 4)

Feature or function	How and why to use it	Reference for more information
Daughter card and channelization support on the 7750 SR	<p>The 5620 SAM supports:</p> <ul style="list-style-type: none"> • Configuring unchannelized 1-port OC192, and 2- and 4-port OC48 daughter cards and card objects. • Configuring channelized 1-port OC12 and the 12-port DS3 daughter cards. You cannot create DS3 children objects using the 5620 SAM. Ports and channels can only be used in access mode. • Configuring BCP-Null, BCP Dot1q, Frame Relay, and IPCP encapsulation on access ports and channels on the daughter cards listed above. • Configuring PPP encapsulation on network ports and channels on the daughter cards listed above. • Configuring channelized 1x OC12 daughter cards and card objects to the DS0 level using the STS1 sub-channels that are available. • Configuring channelized 12xDS3/E3 daughter cards and card objects to the DS0 level using TDM channels. 	See the equipment manager overview and procedural information in chapter 13.
MPLS administrative group policy support	The 5620 SAM supports configuring MPLS administrative group policies, and assigning the groups to MPLS interfaces, LSPs, and LSP paths.	See the MPLS administrative group, MPLS interface, LSP, and LSP path procedural information in chapter 16.
Slope and network policy support	The 5620 SAM supports configuring slope and network policies which can be applied to router objects during service configuration or modification.	See the policy overview and procedural information in chapter 20.
Q in Q support	The 5620 SAM supports enabling Q in Q encapsulation on applicable ports, and configuring Q in Q encapsulation values on interfaces.	<p>See the port and channel procedural information in chapter 14 to enable Q in Q.</p> <p>See the service creation procedural information in the appropriate service management chapter to configure encapsulation value on interfaces.</p>
CSPF, Make before Break, and inheritance support on LSPs and LSP paths	The 5620 SAM supports configuring CSPF and Make before Break parameters on LSPs and LSP paths, and the inheritance of key LSP parameters, including CSPF and Make Before Break, by LSP paths.	See the LSP and LSP path procedural information in chapter 16.
MPLS topology maps, including LSP map	From the GUI, you can view additional maps that show the MPLS and LSP topology.	See the map management information in chapter 27.
Product renaming	The 5620 SRM has been renamed to the Alcatel 5620 Service Aware Manager. The majority of instances of 5620 SRM on the GUI have been renamed.	—

(3 of 4)

Feature or function	How and why to use it	Reference for more information
HVPLS	<p>A hierarchical VPLS is created by enhancing the VPLS core mesh with access spoke circuits that are interconnected to another VPLS, a VLL, or a site.</p> <p>An HVPLS can:</p> <ul style="list-style-type: none"> • reduce the complexity of mesh configuration • decrease the amount of signaling of routes between devices <p>When traffic arrives at an access spoke circuit, it acts similarly to a bridge port. Flooded traffic received on the access spoke is replicated to all other spokes, meshes, or service access points but is not transmitted on the port where it is received.</p>	See the VPLS overview and procedures documentation for information about creating HVPLS spokes in chapter 24.
Grouping	<p>You can use the grouping function to:</p> <ul style="list-style-type: none"> • represent devices that are located in the same area, for example, in the same city • indicate network topology, for example, devices that operate in the same spanning tree or SONET/SDH ring 	See the navigation tree configuration Procedure 14-1 for more information about creating groups.

(4 of 4)

2.5 Basic FAQs to troubleshoot the 5620 SAM

Use the following FAQs to help improve your use of the 5620 SAM. See the *Alcatel 5620 SAM Network Management Troubleshooting Guide* for more information about troubleshooting.

How do I limit the number of reads and writes to the router?

By default, the 5620 SAM activates a save command to the router every time a configuration change is made using the 5620 SAM. You can write changes to the router less often by using the Mediation→Deployment and Site Backup/Upgrade configuration form from the 5620 SAM main menu. Click on the Deployments Policy tab. Set the Auto Save Scheme parameter to Every Nth Deployment. Set the Auto Save Threshold to N , where N is the number of SNMP deployments.

The higher the number, the less often changes are deployed to the router.



Caution — The longer the delay in changes deployed to the router, the greater the risk of a router reboot that will cause you to lose changes.

How should I name objects on the GUI?

Develop a standardized naming conventions to be used by all operators when they configure the network. This will:

- ease identification of the type of object
- ensure that data passed to a northbound OSS interface or southbound in a data file for processing are named consistently across platforms and software products

Name each object on the appropriate configuration form to identify:

- the type of object, for example, a VPLS service
- any customer associations with the object, for example, a VLL service for XYZ Industries
- the source and destination of endpoints, for example, the devices that start and terminate an LSP
- the ports and IP addresses used

For example, to create an Ethernet connection between devices with the names 'top' and 'bottom', using port 24 on each router, use the following name, Top/1/1/1/1 (10.10.10.1/24) to Bottom/1/1/1 (10.10.10.2/24)

You can easily identify that link started on device Top, terminating on device Bottom, and used the specified addressing and ports.

3 — The GUI

- 3.1 GUI overview 3-2**
- 3.2 GUI workflow 3-3**
- 3.3 GUI menus 3-3**
- 3.4 GUI procedures 3-4**
- 3.5 GUI basic operation procedures 3-4**

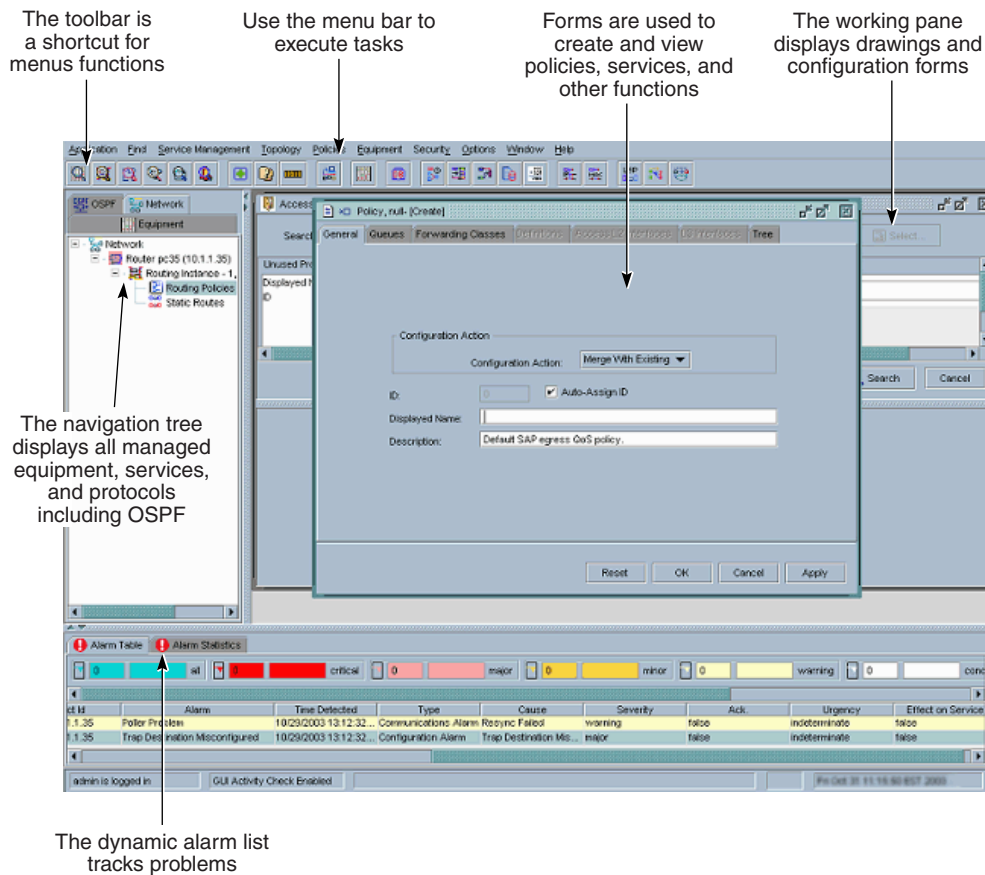
3.1 GUI overview

The 5620 SAM GUI is run from the 5620 SAM client PCs or networkstations. Many clients can connect to the same 5620 SAM server. The GUI is used to provide FCAPS functionality for network operators performing tasks in the network operations centre:

- display equipment and alarm status
- configure and manage network management applications
- simplify the administration and execution of equipment, service, and subscriber configuration using step-based configuration forms instead of the CLI.
- configure, manage, and monitor SLAs and equipment using performance counters
- create and manage security policies for secure access to the routers and for operations using the 5620 SAM

Figure 3-1 shows the main GUI elements.

Figure 3-1 GUI elements



17184

3.2 GUI workflow

- 1 Start the 5620 SAM GUI.
- 2 Set GUI preferences.
- 3 Navigate through the GUI elements.
 - a Navigate using shortcuts from the 5620 SAM menu.
 - b Navigate through the GUI elements related to your job function, for example, the system administration forms.

You can determine which windows and forms are applicable to your job function by checking the appropriate workflow.

- 4 Perform your job function.

3.3 GUI menus

Table 3-1 lists the top level GUI menus and the groups of tasks they contain.

Table 3-1 5620 SAM GUI menus

Menu item or option	Function
Application→Exit	Shut down the 5620 SAM GUI.
Find→ <i>Submenus</i>	List and then browse configured 5620 SAM services, network information, statistics, logs, alarm and database objects.
Service Management→ <i>Submenus</i>	Manage services, customers and FIBs.
Topology→ <i>Submenus</i>	Manage maps and views of the network, including a subscriber view of services used by the customer.
Policies→ <i>Submenus</i>	Configure and manage policies related to alarm handling, quality of service, routing protocols, schedules, ACLs, services, and statistics.
Equipment→Equipment Manager	Configure and manage routers.
Mediation→ <i>Submenus</i>	Configure and manage discovery of network objects.
Security→ <i>Submenus</i>	Configure and manage users and security access.
Options→ <i>Submenus</i>	Numerous functions, including opening a Telnet or SSH session with network equipment.
Window→ <i>Submenus</i>	Manage how forms are displayed in the working pane
Help→ <i>Submenus</i>	Show the splash screen. Splash screen information shown includes the release version of the software and license key information.

3.4 GUI procedures

Table 3-2 lists the GUI-related procedures.

Table 3-2 GUI procedures list

Procedure	Purpose
To start the 5620 SAM GUI from a PC	Start the 5620 SAM client GUI from a PC
To start the 5620 SAM GUI from a Solaris workstation	Start the 5620 SAM GUI from a Solaris workstation.
To disable or enable the GUI activity check	To set up the GUI to user preference to prevent the GUI from closing based on an inactivity counter
To navigate the GUI	Navigate and familiarize users with the GUI layout and major functions
To use menus, the toolbar, or shortcuts	Quick ways to perform tasks
To view and manipulate listed information	Using list and filter forms to change the display of information and to provide inventories of network objects
To save list preferences	Save preferences for the display of listed information
To view software release and license key information	View the build version of the 5620 SAM software and license information
To exit the 5620 SAM GUI	Exit the 5620 SAM GUI

3.5 GUI basic operation procedures

Use the following procedures to perform GUI basic operations.

Procedure 3-1 To start the 5620 SAM GUI from a PC

- 1 Double-click on the shortcut icon that was created on your desktop when the software was installed.

The 5620 SAM login form appears.

Alternately, you can open a command window, navigate to the 5620 SAM client installation directory, and type `nmsclient.bat`.

- 2 Enter your Login Name and Password, and click on the Login button.



Note — If this is the first time that you are logging in, use the admin login. Contact your Alcatel support representative for default account information.

The 5620 SAM GUI opens.

Procedure 3-2 To start the 5620 SAM GUI from a Solaris workstation

- 1 As root in the bash shell, navigate to the appropriate bin directory in the 5620 SAM client installation directory, for example the /nms/bin directory.

- 2 Start the 5620 SAM client by typing:

```
nmsclient.bash ↵
```

The 5620 SAM login form appears.

- 3 Enter your Login Name and Password.



Note — If this is the first time that you are logging in, use the admin login. Contact your Alcatel support representative for default account information.

- 4 Click on the Login button.

The 5620 SAM GUI opens.

Procedure 3-3 To disable or enable the GUI activity check

By default, the 5620 SAM client times out after 15 min of inactivity. You can disable this functionality by choosing Security→Disable GUI Activity Check from the main menu. You can enable this functionality by choosing Security→Enable GUI Activity Check from the main menu.

Procedure 3-4 To use menus, the toolbar, or shortcuts

- 1 Open the 5620 SAM GUI.
- 2 Choose a menu:
 - a From the drop-down submenu options under each top-level menu, as shown in Table 3-1. An applicable shortcut icon for the menu item is shown next to the option text.
 - b From the menu equivalent in the toolbar. Scroll over the icons to view their function.

- c By typing the appropriate ALT+Key shortcut. For example, ALT+P opens the policies menu. The underlined letter indicates the shortcut action.
-

Procedure 3-5 To navigate the GUI

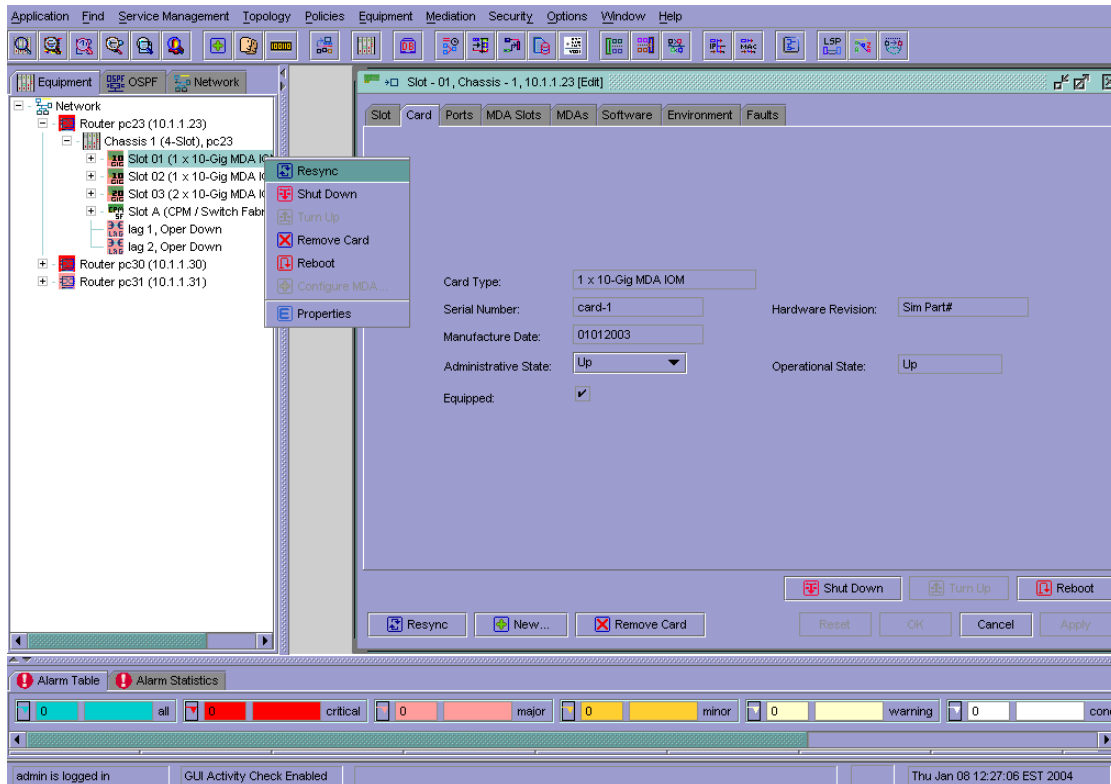
- 1 Open the 5620 SAM GUI.
 - 2 Navigate through the main GUI elements, as shown in Figure 3-1.
 - i The menu bar organizes tasks under broad headings.
 - ii The working pane displays windows, drawings, and configuration forms.
 - iii The navigation tree contains the managed equipment, services, and IP network protocols.
 - iv The dynamic alarm list displays incoming events and alarms.
-

Procedure 3-6 To use windows, drawings, and forms to set or view parameters

- 1 Open the 5620 SAM GUI.
- 2 Open a configuration form or window by:
 - choosing the appropriate menu option or submenu option from the 5620 SAM main menu, as listed in Table 3-1
 - double-clicking on an appropriate object, for example a subscriber from a list of subscribers
 - right-clicking on an applicable object and choose the appropriate option from the contextual menus, for example, right-clicking on a managed router in the navigation tree window to view its contextual menu and choosing an option

For example, when right-clicking on a router in the navigation tree, a contextual menu appears, as shown in Figure 3-2. To view the contextual menu options, scroll down the list and choose the appropriate option. The appropriate window or configuration form appears.

Figure 3-2 Right-click contextual menu example



3 View the configuration form or window in the working pane.

Some configuration forms take you through a series of configuration screens. As shown in Figure 3-3, you complete each of the tasks in sequence and click on the Next button to continue configuration, until the task is complete. This figure shows that step 1 is complete, and step 2 is highlighted to show it is being performed. When the task is done, you click on the Finish button. Each of the steps must be completed, or the defaults accepted, before the full task is complete.



Note — Some steps may open a new configuration form. Complete the steps in the new configuration form. When you click the Finish or OK buttons, as appropriate, the previous configuration form reappears.

Figure 3-3 Example of a configuration form with multiple steps

Define Service Type

Service ID: Auto-Assign ID

Service Name:

Description:

Type:

- 4 Set or view the parameters for the configuration form using the following methods:



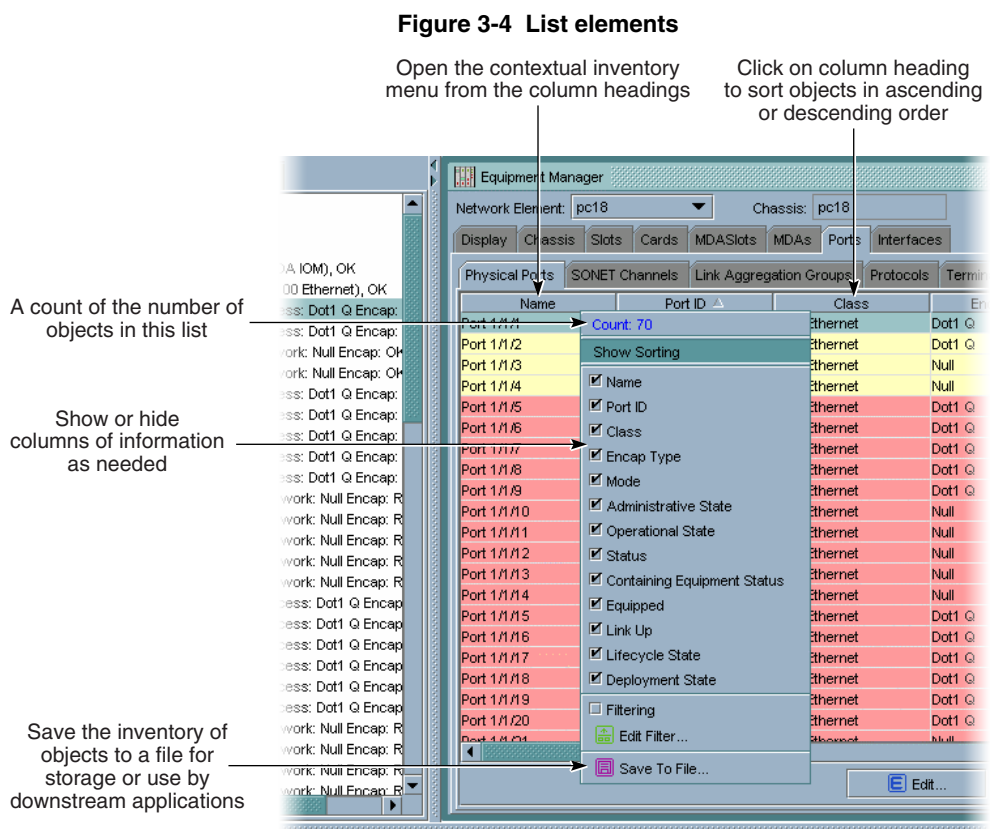
Note — Parameters highlighted in yellow are mandatory and must be set for the task or function to work.

- a Type information next to the parameter, as appropriate. For example, enter text to provide a description for the Description parameter.
 - b Use the drop-down menu to choose an option from a list. For example, choose access as the port mode from a port configuration form.
 - c Follow the form prompts as directed, as described in step 3.
 - 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 to display additional contextual menu choices, as shown in Figure 3-2.
 - f Set the appropriate parameters.
- 5 Click on appropriate button to complete the configuration:
- a The OK or Apply button to save the changes, as appropriate based on the configuration form.
 - b The Reset button to return to the last saved configuration.
 - c The Turn Up button to turn up the object being configured.
 - d The Shut Down button to shut down the object.

- e The Cancel button to close the form or window without saving the changes.
- f The Resync button to ensure that the 5620 SAM and the managed devices are synchronized. Resynchronization does not impact the contents of the historical statistics database.

Procedure 3-7 To view and manipulate listed information

Many of the windows and forms shown in the application pane are lists of network objects. For example, lists of ports from the equipment manager, displaying all the ports on a particular card. Figure 3-4 shows the major elements of a list.



17271

You can manipulate most lists to:

- generate inventories of the listed data
- reorganize the information from most important to least important
- remove columns of data not of interest
- sort 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 and view the number of objects in the list.
 - b To reorganize the information, right-click on a column and drag the column to another location.
 - c To remove columns, right-click on the column and deselect the column from the check mark list. The column disappears from the display.
 - d To sort in ascending or descending order, click on the column heading. The arrow direction changes, indicating if the data is sorted in descending (down arrow) or ascending (up arrow) order.
-

Procedure 3-8 To save list preferences

You can save the format of a list. When you generate the list, it automatically appears in the format saved.

- 1 Perform Procedure 3-7.
 - 2 Right-click on the list and choose Save Table Preferences.

A dialog box appears to confirm that you want to save the current table format.
 - 3 Click on the Yes button.

The table format is saved.
-

Procedure 3-9 To view software release and license key information

View the software release build and license key information from the splash screen.

- 1 Choose Help→About from the 5620 SAM main menu.

The splash screen appears.
 - 2 Review the software release information.
 - The build information specifies the release of the 5620 SAM software installed, for example SAM Release 2.0 R1, where 2.0 is the release number, and R1 is the first hardened load.
 - The license key information specifies the licensed daughter card support limit and the number of daughter cards currently managed by the 5620 SAM.
 - 3 Click on the Close button to close the splash screen.
-

Procedure 3-10 To exit the 5620 SAM GUI

Choose Application→Exit from the 5620 SAM main menu.

The GUI and application closes.

4 — Form management

- 4.1 Forms overview 4-2**
- 4.2 Forms management workflow 4-3**
- 4.3 Forms management procedures list 4-3**
- 4.4 Window menu options 4-4**
- 4.5 Form management procedures 4-4**

4.1 Forms overview

5620 SAM forms are used to:

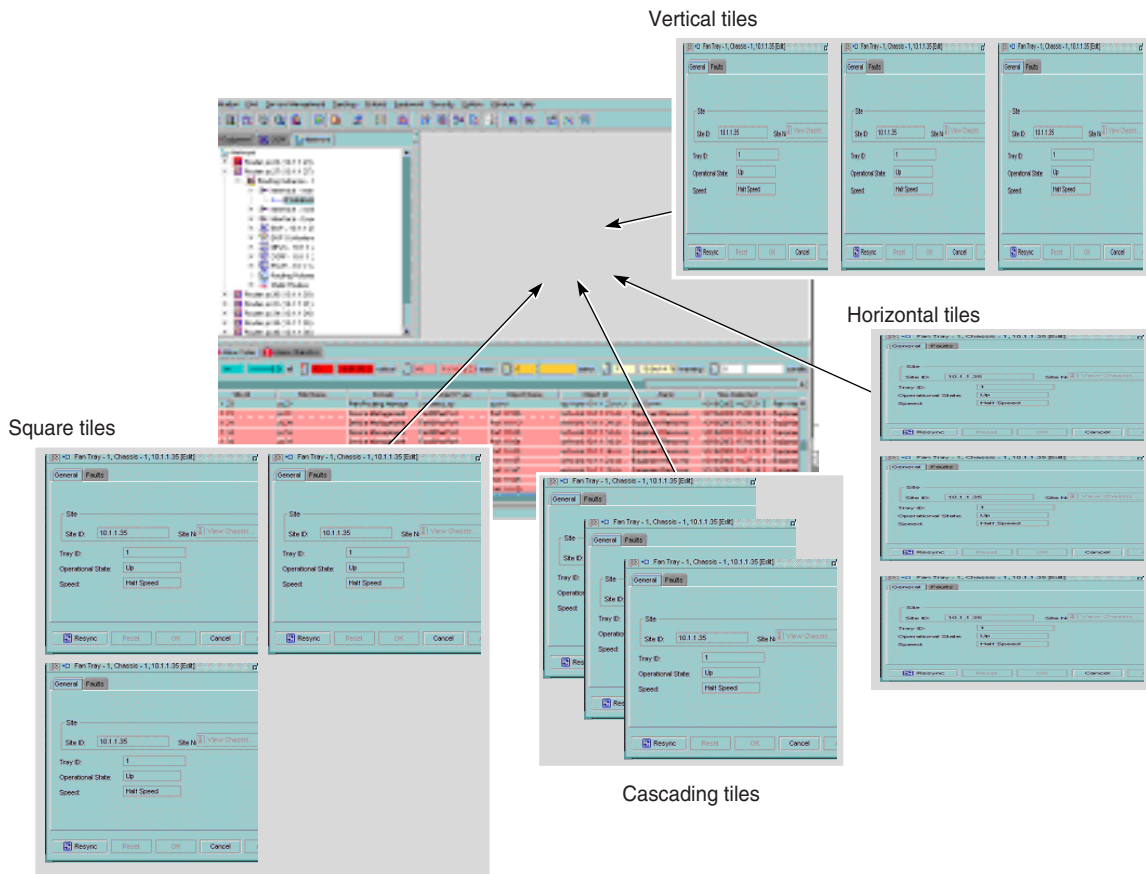
- set configurations on configuration forms
- display drawings and settings
- perform tasks

All 5620 SAM forms, sometimes referred to as windows, are displayed in a working pane on the GUI, to the right of the navigation tree. Each newly opened form appears in the foreground. The previously opened form is placed in the background. The working pane can contain other configuration forms, drawings, maps, and displays. With form management you can:

- organize forms according to operator preference
- keep forms open until they are needed
- perform side by side comparisons of data on different forms
- navigate quickly to other open forms using a numbered list, which is ordered according to the time that the form was opened

Figure 4-1 shows the different ways that forms can be organized to promote efficient workflow and quick access to all necessary information.

Figure 4-1 Form tiling formats



17168

4.2 Forms management workflow

- 1 Open the appropriate forms. See the appropriate chapter or section for the tasks to be performed.
- 2 Manage the open forms in the working pane to maximize operator effectiveness and efficiency.
 - a Bring the form on which you want to work to the foreground.
 - b Organize the location and appearance of open forms.
- 3 Close unnecessary forms to clear the working area pane.

4.3 Forms management procedures list

Table 4-1 lists the procedures to perform forms management tasks.

Table 4-1 5620 SAM forms procedures list

Procedure	Purpose
To arrange forms in the working pane	Organize forms to maximize efficiency
To bring an open form to the foreground	Bring a form needed to complete a task to the foreground on the GUI.
To close forms	Close one or all open forms

4.4 Window menu options

Table 4-2 lists the Window menu options and the function of each menu option.

Table 4-2 5620 SAM window menus

Menu option	Function
Reset to Preferred Sizes	Reset the form in the foreground to the default size.
Cascade & Reset to Preferred Sizes	Reset the form in the foreground to the default size and cascade.
Close All	Close all open forms
Minimize All	Reduce all forms to a small rectangle with truncated titlebar title.
Tile Vertical Tile Horizontal Tile Square Tile Cascade No Arrange	Use the radio button to choose a method of tiling open forms.
<i>Open form 1</i> <i>Open form 2</i> <i>Open... etc.</i>	Use the radio button to choose the form you want to bring to the foreground. The radio button is selected for the form currently in the foreground.

4.5 Form management procedures

Use the following procedures to perform form management tasks.

Procedure 4-1 To arrange forms in the working pane

- 1 Open the Window menu drop-down list.
The menu options appear.
- 2 Use the Tile menu options to organize the open forms by preference and efficiency.

Figure 4-1 shows the tiling options.

Procedure 4-2 To bring an open form to the foreground

- 1 Open the Window menu drop-down list.
The menu options appear.
 - 2 Click the radio button to choose an open form from the list at the bottom of the menu.
The form moves to the foreground.
-

Procedure 4-3 To close forms

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

Choose Close All from the Window menu to close all open forms.

5 — Search and find functions

- 5.1 Performing searches overview 5-2**
- 5.2 Performing searches workflow 5-2**
- 5.3 Performing searches menu 5-2**
- 5.4 Performing searches procedures list 5-3**
- 5.5 Performing searches procedures 5-3**

5.1 Performing searches overview

The 5620 SAM Find menu enables you to search for:

- subscribers
- services
- service tunnels (also called SDPs)
- SAPs

Once you perform a search, you can view or edit subscriber account information, add services, change service parameter values, delete a service or account, and log records.

Searches can be performed using the Find menu, by clicking on the Search button, or by clicking on the Select button in a 5620 SAM form. You can perform advanced or simple searches. Only simple searches are described in this chapter.

When you use the Find menu to perform a search, a browse form appears. The form contains buttons, check boxes, and filter options to refine the search criteria.

5.2 Performing searches workflow

- 1 Start the search:
 - a Choose the appropriate Find menu option from the 5620 SAM main menu.
 - b Click on the Search button or Select button from the appropriate form.
- 2 Configure the search filter parameters if required.
- 3 Click on the OK button.

The results of the search are displayed.

5.3 Performing searches menu

Table 5-1 lists and describes the Find menus.

Table 5-1 5620 SAM Find menu options

Menu item	Description
Find→Browse Equipment	Search for equipment including slots, cards, and ports.
Find→Browse Routing Instances	Search for specific routing instances.
Find→Browse MPLS	Search for specific MPLS information across multiple devices.
Find→Browse Services	Search for VLL, VPLS, and IES services.
Find→Browse Log Records	Search for log records and view statistics information.
Find→Browse Alarm History	Review historical alarms for trends.

5.4 Performing searches procedures list

Table 5-2 lists and describes the procedures to perform a search.

Table 5-2 5620 SAM search procedures list

Procedure	Purpose
To perform a simple search from the Find menu	Find equipment, routing instances, MPLS, services, log records, and historical alarm information.
To perform a search using the Search button	Find entries in a 5620 SAM form, including FIB, service tunnel, MPLS, and LSP entries.
To perform a search using the Select button	Find policies, subscribers, IDs, and other entities in a 5620 SAM wizard.

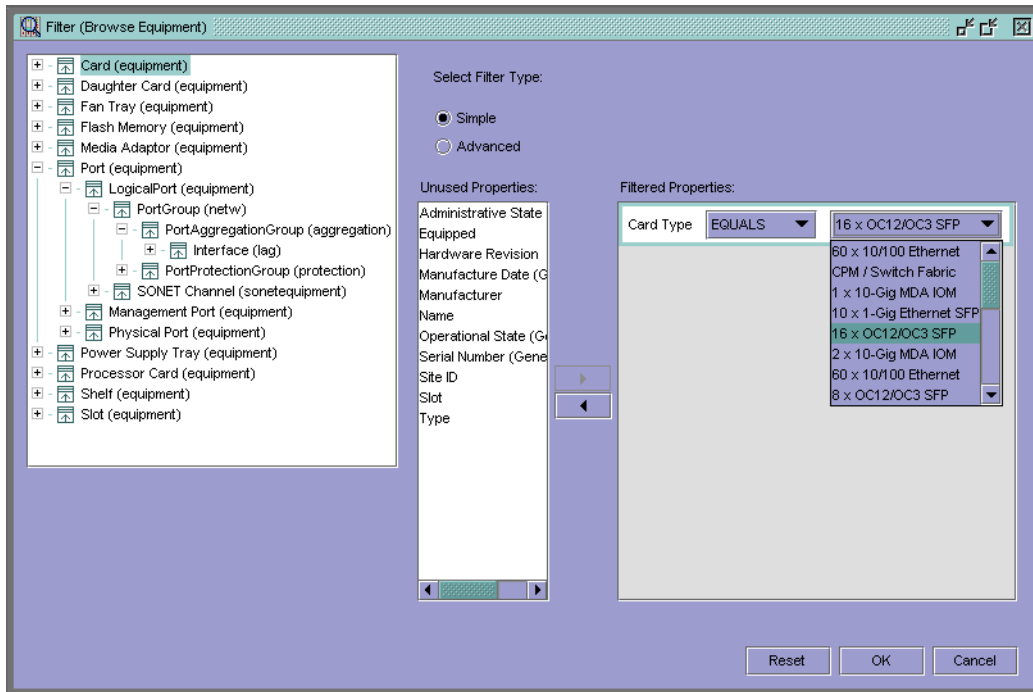
5.5 Performing searches procedures

Use the following procedures to perform 5620 SAM searches.

Procedure 5-1 To perform a simple search from the Find menu

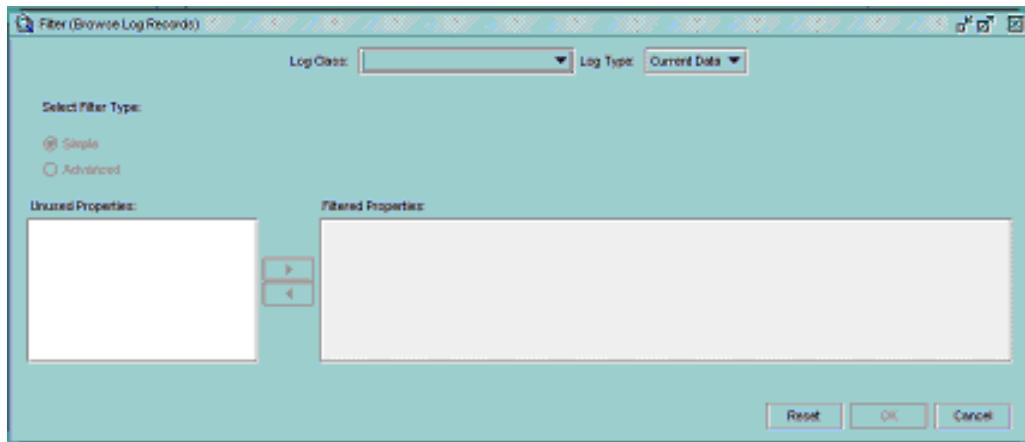
- 1 Choose the appropriate Browse menu item from the Find menu.
 - a Use the Filter form shown in Figure 5-1 to search for equipment, routing instances, MPLS, alarms, or services. The Browse form appears behind the Filter form. Go to step 4.

Figure 5-1 Filter (Browse Equipment) form



- b** Use the Filter form shown in Figure 5-2 to search for log records. The Browse form appears behind the Filter form.

Figure 5-2 Filter (Browse Log Records) form



- 2** Choose an item from the Log Class drop-down menu.
A list of parameters is displayed in the Unused Properties box.
- 3** Choose an item from the Log Type drop-down menu.
- 4** Configure the filter parameters.
 - i** Click on or navigate to the item that you want to perform the search on in the Unused Properties box on the left side of the form.

A list of parameters is displayed in the Unused Properties box. Leaving fields blank in the Filtered Properties box results in an any or all type of search. For example, if you are filtering on equipment, and you do not specify any equipment parameters in the Filtered Properties box, the search process returns a list of all available equipment. For fields that provide a pull-down list of options, the Unknown option is also used as an any or all type of search criteria.

- ii Ensure that the Simple radio button is chosen.
- iii Click on the property or properties that you want to filter your search on and click on the right arrow button.

The properties are moved to the Filtered Properties box.

- iv Set the search parameters for each property in the Filtered Properties box.
- 5 Click on the OK button.

The Filter form closes and the appropriate Browse form appears listing the results of your search.

- 6 Choose an item from the results list and click on the Edit button to view or configure the parameters if required.
- a Click on the Edit Filter button to reset the search parameters.
 - b Click on the Refresh button to refresh the search.
 - c Click on the Close button to close the form.
-

Procedure 5-2 To perform a search using the Search button

Use the following procedure to find entries in a 5620 SAM form, including FIB, service tunnel, MPLS, and LSP entries. Many of the forms display the Search button. The Search button can be used instead of the Find menu. You can filter properties to refine your search or click on the Search button to perform an any or all type of search.

- 1 Configure the search parameters in the appropriate form. For example, use the Search Filter Type drop-down menu to specify the search type, or deselect the Any Source check box to pick a source IP address as the search filter.

Figure 5-3 shows a sample form with a Search button.

Figure 5-3 LSP Manager form showing Search button

The screenshot shows the LSP Manager application window. At the top, there is a 'Search Filter Type' dropdown menu set to 'Endpoints'. Below this, there are two sections: 'Source' and 'Destination'. Both sections have a checked checkbox for 'Any Source' and 'Any Destination' respectively. Each section contains a table with columns for 'Site ID', 'Site Name', 'Name', and 'System I'. The 'Source' table lists three entries: (10.1.1.23, pc23, pc23, 10.1.1.2), (10.1.1.27, pc27, pc27, 10.1.1.2), and (10.1.1.34, pc34, pc34, 10.1.1.3). The 'Destination' table lists the same three entries. At the bottom right of the form, there is a 'Create LSP...' button and a 'Search' button. An arrow points to the 'Search' button with the label 'Search button'. Below the buttons, there is a large empty area with the text 'Setup a filter to find your LSPs and click "Search."'.

17192

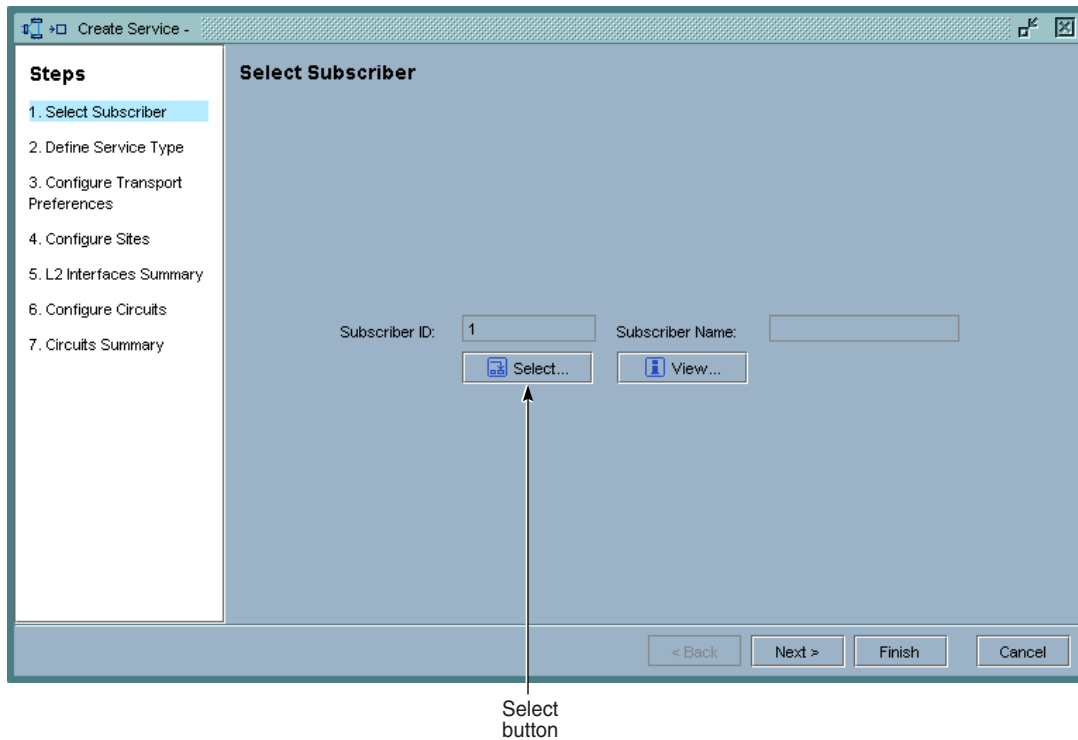
- 2 Click on the Search button.
Search results appear in the bottom panel of the form.
- 3 Choose an item from the results list and click on the Edit button to view or configure the parameters if required.
 - a Click on the Edit Filter button to reset the search parameters.
 - b Click on the Refresh button to refresh the search.
 - c Click on the Close button to close the form.

Procedure 5-3 To perform a search using the Select button

Use the following procedure to find policies, subscribers, IDs, and other entities in a 5620 SAM series of configuration forms. The Select button appears as an option in the 5620 SAM configuration forms. Use this button to search for and display valid options for a selection.

- 1 Click on the Select button in the configuration form. Figure 5-4 shows a sample service configuration form with a Select button.

Figure 5-4 Sample service configuration form with Select button



17193

A filter form opens.

- 2 Click on the Simple radio button.
- 3 Click on the property or properties that you want to filter your search on from the Unused Properties box and click on the right arrow button.

The selected properties are moved to the Filtered Properties box.

- 4 Set the search parameters for each property in the Filtered Properties box.
- 5 Click on the OK button.

The Select form displays the results of the search.

- 6 Double-click on an entry to select it.

The Select form closes and the entity information appears in the configuration for form.

For example, as shown in Figure 5-4, the subscriber with ID 1 was selected from the search results for this step in the procedure.

Discovering routers and administering the network

- 6 — Discovery manager**
- 7 — In-band and out-of-band management**
- 8 — Security management for 5620 SAM groups and users**
- 9 — Security management for 7750 SR users with RADIUS or TACACS+**
- 10 — Deployment and site backup/upgrade management**
- 11 — 5620 SAM database manager**
- 12 — Using CLI from the 5620 SAM**

6 — *Discovery manager*

- 6.1 Network element discovery overview 6-2**
- 6.2 Discovery workflow 6-3**
- 6.3 Discovery menus 6-3**
- 6.4 Discovery procedures list 6-3**
- 6.5 Discovery procedures 6-4**
- 6.6 SNMP MIBs 6-18**

6.1 Network element discovery overview

The 5620 SAM simplifies network provisioning by allowing you to discover devices and reconcile them to the 5620 SAM database for management.

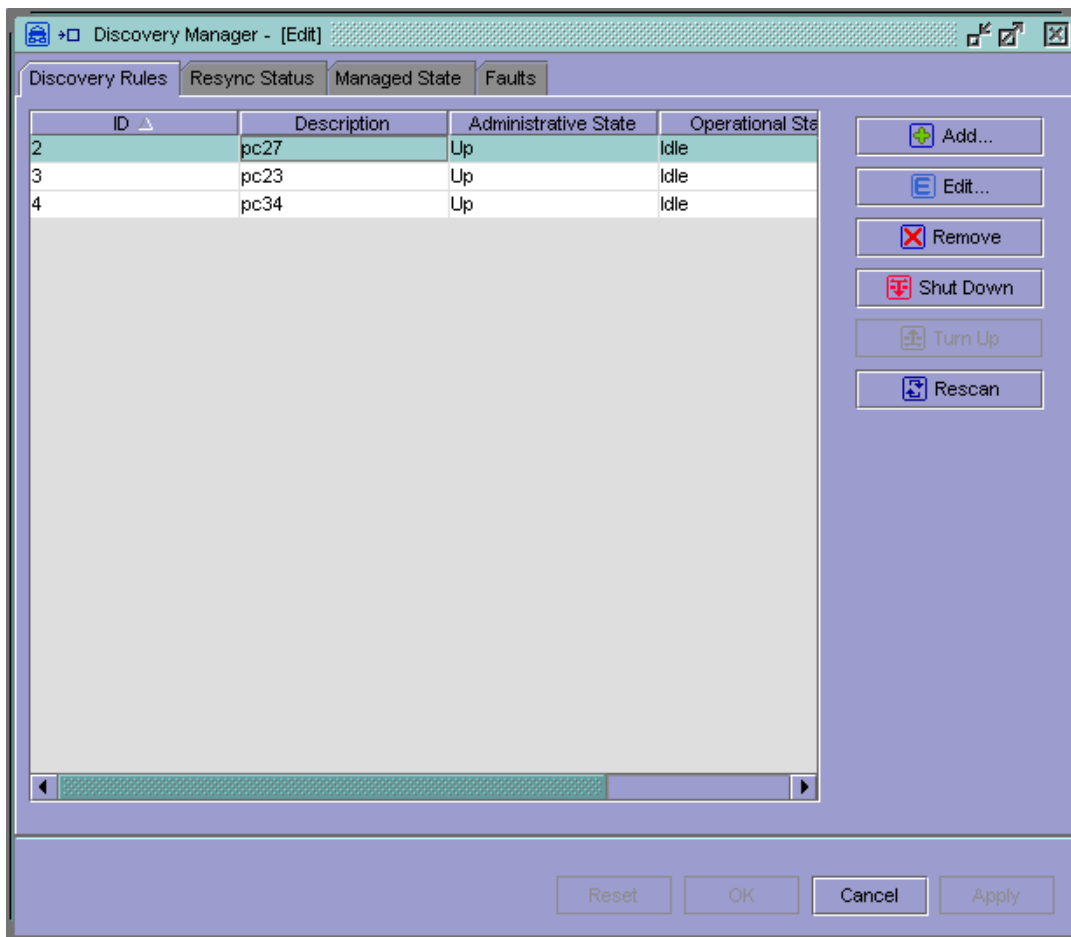
Network element discovery is executed via SNMP. During the discovery process, the 5620 SAM scans the network for devices according to user-defined IP addresses or IP address ranges. When a device is discovered, the 5620 SAM sets the device in a managed state and reconciles device elements into the 5620 SAM database.

To discover devices, you use the Discovery Manager to create one or more discovery rules, choose a discovery rule, and scan the network as specified by the rule.

Discovery rules contain rule elements. Rule elements specify which devices or subnets are to be included in or excluded from the discovery process. A discovery rule can contain more than one rule element. For example, you can configure one rule element to discover a subnet, and configure another rule element to exclude specific IP addresses from the subnet.

Figure 6-1 shows a Discovery Manager form with the Discovery Rules tab button selected.

Figure 6-1 Discovery Manager form - Discovery Rules



6.2 Discovery workflow

The following workflow outlines the high-level steps necessary to discover the network.

- 1 Using the CLI, configure the SNMP security parameters on the devices that you want to discover.
- 2 Configure poller policies.
- 3 Discover devices.
 - Create discovery rules
 - Discover devices by scanning the network according to discovery rules
 - Set discovered device in a managed state
 - Reconcile device elements into the 5620 SAM database
 - Check discovery, management, and reconciliation status of the devices
- 4 Manage the device discovery.
 - Edit discovery rules
 - Add or edit rule elements
 - Enable or disable discovery rules
 - Remove discovery rules
 - Rescan the network according to a discovery rule
 - Manage or unmanage devices
 - Reconcile device elements into the 5620 SAM database

6.3 Discovery menus

Table 6-1 lists the discovery menu items.

Table 6-1 5620 SAM discovery menus

Menu item	Task
Mediation→Discovery Manager	Access the discovery manager form to discover and reconcile routers.
Mediation→Poller Policies	Configure the 5620 SAM to poll network elements at regular intervals.

6.4 Discovery procedures list

Table 6-2 lists the discovery procedures.

Table 6-2 5620 SAM discovery procedures list

Procedure	Purpose
To configure poller policies	To configure the 5620 SAM to poll network elements at regular intervals
To configure polling policies and discovery to use SNMPv3	To configure the 5620 SAM to use SNMPv3 for secure network element polling
To discover devices	<ul style="list-style-type: none"> • Create discovery rules • Discover devices by scanning the network according to discovery rules • Set discovered devices in a managed state • Reconcile router elements into the 5620 SAM database • Check discovery, management, and reconciliation status of router
To edit a discovery rule	To edit a discovery rule to specify a change to the way devices are scanned
To enable or disable a discovery rule	To enable or disable a discovery rule
To remove a discovery rule	To remove a discovery rule
To rescan the network according to a discovery rule	To rescan a the network according to a discovery rule, for example, if the initial discovery attempt fails
To manage or unmanage a device	To manage or unmanage a device
To reconcile device elements in the 5620 SAM database	To reconcile router elements, for example if the initial reconciliation fails

6.5 Discovery procedures

This section provides discovery procedures.

Procedure 6-1 To configure poller policies

Perform this procedure to configure the 5620 SAM to poll network elements at regular rates and intervals.

- 1 Choose Mediation→Poller Policies from the 5620 SAM main menu.
The poller manager form appears.
- 2 Click on the General tab button.

- 3 Configure the parameters.
 - i Specify the Base Polling Interval parameter to specify how often all device MIB elements of discovered and managed devices are polled for changes to their MIBs. Any change to the MIB triggers the 5620 SAM to re-read the entire MIB and update its database. You can choose a range of 5 minutes to 48 hours, depending on network needs.
 - ii Specify the Discovery Rule Scan Interval parameter to specify how often the 5620 SAM rescans the network according to previously enabled discovery rules. You can choose a range of 5 minutes to 48 hours, depending on network needs.



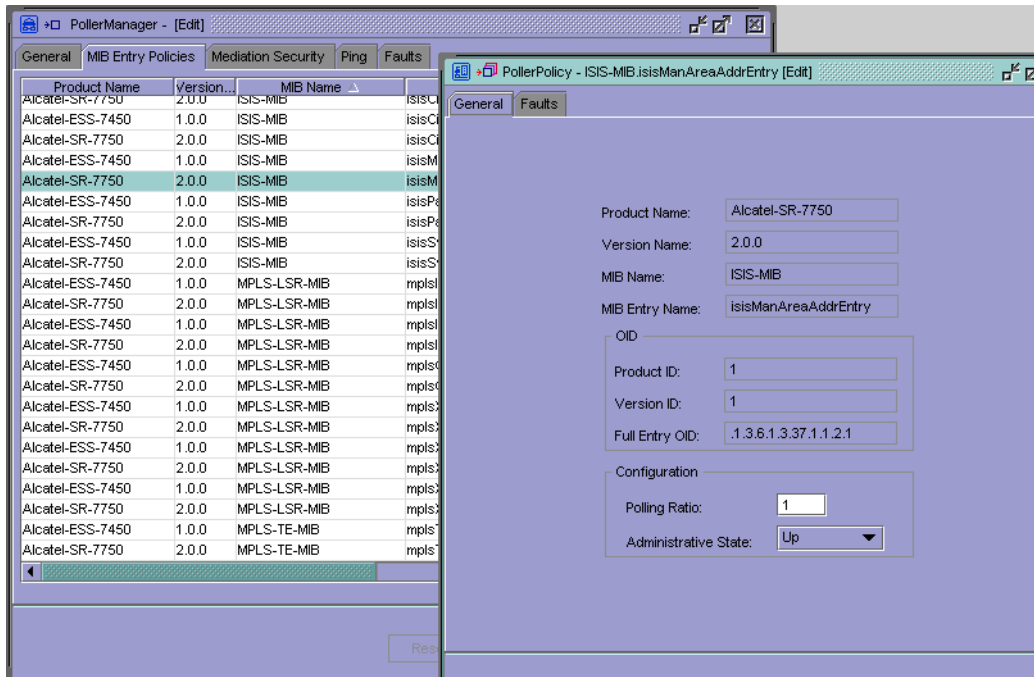
Note — Polling and scanning use system resources, and can increase the amount of management traffic. Consider your network needs and network management domain capabilities when setting these parameters.

- 4 Configure additional parameters, as required.
 - i You can specify different polling ratios for different MIBs. Click on the MIB Entry Policies tab button to edit MIB entry policies.

A list of MIBs appears, organized by the product name of the device that supports the MIB.
 - ii Select one or more MIBs from the list.
 - iii Click on the Edit button to specify a different polling ratio for a MIB or MIBs.

The poller policy form for that MIB appears as shown in Figure 6-2.

Figure 6-2 MIB entry poller policy form - General



- iv Specify the Polling Ratio parameter. For example, if the Base Polling Interval parameter is set to poll every 12 hours, you can then set the Polling Ratio parameter for a specific MIB to 2. This means the specified MIB is polled once in two times the interval, or every 24 hours. See Table 6-3 for a list of MIBs and MIB entries.
 - v Set the Administrative State parameter to Up to enable polling of the MIB.
 - vi Click on the OK button to save the changes.
- 5 Click on the Mediation Security tab button to specify SNMP security settings. To configure SNMPv3 security, you must perform configurations on the 5620 SAM server, the managed devices, and using GUI configuration forms. See Procedure 6-2 for more information.
- i Click on the Add or Edit buttons to create or change SNMP mediation security policies.
 - ii Specify a name for the mediation policy using the Displayed Name parameter.
See chapter 9 for more information about managed device account configuration and management.
 - iii Set the Security Model parameter to the version of SNMP used for security.
When you set the security model to SNMP V2, you have to configure the Community String parameter. The community string should match the community string set of the managed element.

When you set the security model to SNMP v3 (USM), you are prompted to assign a user profile that has been configured with the SNMP v3 authentication and privacy parameters, as described in Procedure 6-2.

- Click on the Select button to view a list of configured users. The Select Site User For SNMP Access form appears.
 - Select a user from the list and click on the OK button. The user name appears.
 - Click on the View button to view the configuration details of the user's permissions and SNMP v3 security settings.
- 6** Click on the Ping tab button to define how the management IP addresses of devices are checked using a ping. Each managed device provides the following three IP addresses that can be scheduled to be pinged:
- the system IP address, called an in-band management interface
 - the management IP address, called an out-of-band management interface
 - the IP address of the standby Control card, also called a CPM
- i** One default ping policy is available. To edit the existing policy, click on the Edit button. To create a new policy, click on the Add button.
 - ii** The ManagementPingPolicy form appears. Specify the parameters for the ping policy.
 - iii** Specify the Displayed Name parameter to provide a name for the policy.
 - iv** Specify the Ping OS command to define the operating system-specific ping command, replacing \$IP with the IP address target of the ping command.
 - v** Specify the Ping Command Timeout parameter to indicate how long the 5620 SAM waits to complete the ping before declaring a timeout alarm.
 - vi** Select the Schedule Enabled check box to set a regular schedule of pings. Use the ping interval minute and seconds parameters to schedule the ping. You can also perform an unscheduled ping from the Managed State tab of the Discovery Manager configuration form. See Procedure 6-3 for more information.
 - vii** Click on the Ping Destinations tab button. Add or edit the in-band and out-of-band IP addresses for the managed devices that can be pinged.
 - viii** Click on the Apply button to save the changes.
- The 5620 SAM generates alarms if the ping fails:
- the PingPolicyMisconfigured alarm indicates that the ping command or the ping policy settings are invalid
 - the ConnectionDown alarm indicates that the pinged management interface is unreachable
- 7** Click on the Apply button to save the changes.
-

Procedure 6-2 To configure polling policies and discovery to use SNMPv3

SNMPv3 security is designed for user-based security, comprised of secure authentication and communication. The access granted is restricted to the scope of the configured users and groups.

To enable SNMPv3 using the 5620 SAM GUI, the following high-level steps are required:

- generating MD5 and DES keys
- setting up SNMPv3 groups and users on the managed devices
- setting up SNMPv3 users on the 5620 SAM

- 1 Unmanage any existing devices using SNMPv2c security using the discovery manager.
- 2 Delete or modify any discovery rules that use SNMPv2c security to remove the devices that will be modified to use SNMPv3 security.
- 3 Create MD5 security keys using the password2key utility on the 5620 SAM server.
 - i Go to the *install_directory/nms/bin* directory or folder on the 5620 SAM server.
 - ii Run the password2key.bat or .bash utility:


```
password2key MD5 trial snmp_engine_ID_PE1 ↵
```

where
trial is an example of a password
snmp_engine_ID_PE1 is the SNMP engine ID of the managed device using SNMPv3
 - iii Repeat for the number of keys necessary for your security model.
 - iv Store the generated keys.
- 4 Configure SNMPv3 groups and users on the managed devices. The following shows configuring a read user and a read-write user on the 7750 SR.

- i Log in to the 7750 SR.
- ii Create a read-write group:


```
configure system security snmp access group snmpv3_groupname
security-model usm security-level privacy read iso write iso
notify iso ↵

configure system security user snmpv3_username ↵

access snmp ↵

snmp ↵

authentication md5 insert_MD5_authentication_key privacy
des-key insert_DES_privacy_key group snmpv3_groupname ↵
```
- iii Create a read-only group by including only the read iso reference in the CLI command.

- 5 Create SNMPv3 users from the 5620 SAM GUI using the site user manager. See Procedure 9-3 in chapter 9 for more information about configuring site users. Ensure that the following is configured:
 - two users are created, one with write access and one with read-only access
 - give both users SNMP access
 - from the SNMPv3 tab button, use MD5 as the authentication protocol and DES for the privacy protocol
 - type in the appropriate MD5 authentication and DES privacy keys
- 6 Create a new SNMPv3 mediation security policy, as described in Procedure 6-1.
- 7 Create new discovery rules to use SNMPv3 mediation, and choose the write only and read-only users when prompted.
- 8 Rediscover the devices, as required.

Procedure 6-3 To discover devices

Perform this procedure to complete the following tasks:

- Create discovery rules
- Ping the managed devices to test connectivity
- Discover devices by scanning the network according to discovery rules
- Set discovered devices in a managed state
- Reconcile router elements into the 5620 SAM database
- Check discovery, management, and reconciliation status of device



Note — SNMP parameters must be correctly specified on the 7750 SR. Contact your Alcatel support representative for more information.

- 1 Choose Mediation→Discovery Manager from the main menu.
The Discovery Manager form appears.
- 2 Configure a discovery rule.
 - i Click on the Discovery Rules tab button.
 - ii Click on the Add button to create a new discovery rule.
The Create Discovery Rule form appears.
 - iii Configure the parameters in the Specify General Attribute form, as shown in Figure 6-3.

Figure 6-3 Specify general attribute form - Specify General Attribute form

The screenshot shows a window titled 'Create Discovery Rule - [0]' with a 'Specify General Attributes' form. On the left, a 'Steps' sidebar lists: 1. Specify General Attributes (highlighted), 2. Add Rule Elements, 3. Configure Mediation Security, and 4. Configure Management Ping Policy. The main form area contains:

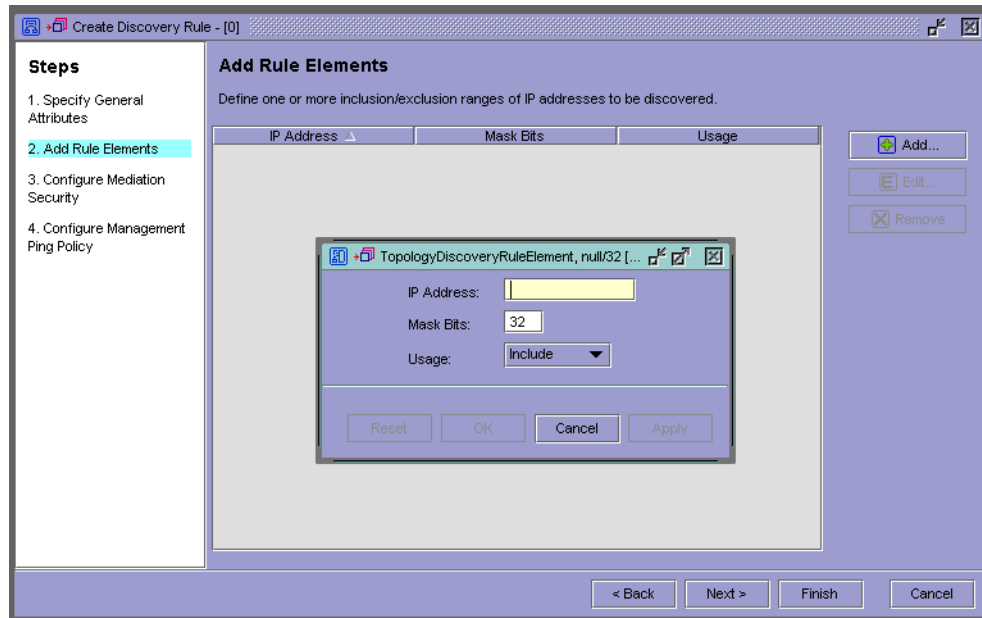
- ID:** A text box containing '0' and a checked checkbox labeled 'Auto-Assign ID'.
- Description:** An empty text box.
- Administrative State:** A dropdown menu currently set to 'Up'.

 At the bottom right, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

- iv** Uncheck the Auto-Assign ID check mark box if you want to specify an ID for the discovery rule. If you unchecked the Auto-Assign ID check mark box, specify an ID for the discovery rule. The range is 1 to 100.
- v** Specify a description for the discovery rule that is up to 80 characters using the Description parameter.
- vi** Specify the Administrative State parameter. 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 poller manager form. When you set the administrative state to Down, the network is not scanned as specified by these conditions.
- vii** Click the Next button.
The Add Rule Elements form appears.
- viii** In the Add Rule Elements panel, click the:
 - Add button to add a new rule element.
 - View button to view and modify the existing default policy.
 - Row representing a rule.
 - Finish button to keep the existing default policy.

When you click on the Add or Edit button, the rule element form appears, as shown in Figure 6-4.

Figure 6-4 Create Discovery Rule form - Add Rule Elements form



- ix** Configure the parameters for the rule element form.
- Specify the management IP address of a device using the IP Address parameter.
 - Specify the mask bits for the IP address of a device using the Mask Bits parameter. You can discover a subnet by specifying a general IP address and setting a portion of the network mask bits to 0. For example, when you set the IP address to 192.168.24.0 and set the network mask bits to 24, all devices in subnet 192.168.24 are discovered.
 - Specify whether you want to include or exclude the IP address or range to in the discovery using the Usage parameter. For example, one rule element may specify that a subnet be included and therefore discovered, while another rule element may specify that specific IP addresses in the subnet be excluded and therefore not discovered.
- x** Click the OK button.
- The discovery rule is saved and the network be scanned according to the discovery rule when you click on the Apply button in the discovery manager form in step 3.
- xi** Add more rule elements as required by performing substeps viii to x.
- xii** Click the Next button.
- The Configure Mediation Security form appears.
- xiii** Specify the mediation policies for read access and write access.
- Click on the Select button if you want to specify mediation security policies specific to the discovery rule. Mediation policies are created or modified using the poller policies form, as described in Procedure 6-1.

If you do not specify a policy, the default policy is applied. Click the Next button.

If you clicked the Select button, the Configure Mediation Security form appears. You can:

- Select an existing mediation security policy from the list and click the OK button.
- Select an existing mediation security policy and click on the Edit button. When you click on the View button, a Mediation Policy (Edit) form appears.
- Set the security model parameter to the version of SNMP used for security.
- When you set the security model to SNMP V2c, you have to configure the community string to match the community string on the managed element. Click on the OK button.
- When you set the security model to SNMP v3 (USM), you are prompted to assign a user profile that has been configured with the SNMP v3 authentication and privacy parameters.
 - Click on the Select button to view a list of configured users. The Select Site User For SNMP Access form appears.
 - Select a user from the list and click on the OK button. The user name appears.
 - Click on the View button to view the configuration details of the user's permissions and SNMP v3 (USM) security settings.
 - Click on the OK button to save the changes.

xiv Click on the OK button to save the changes.

xv Click on the Next button.

The Configure Management Ping Policy form appears.

xvi Specify the management ping policies for each of the following management IP addresses:

- the system IP address, called an in-band management interface
- the management IP address, called an out-of-band management interface
- the IP address of the standby Control card, also called a CPM

The management ping policies are created using the poller manager configuration form. See Procedure 6-1 for more information. Figure 6-5 shows the configure management ping policy parameters on the Create Discovery Rules form.

Figure 6-5 Create Discovery Rule form - Configure Management Ping Policy form

xvii Click on the Select button for each ping policy ID parameter.

The Configure Management Ping Policy list form appears.

xviii Choose a ping policy from the list.

xix Click on the OK button.

The ping policy ID appears in the Policy ID parameter.

xx Click on the Finish button.

3 Save the discovery rule, and discover devices by scanning the network as specified by the discovery rule.

i Click on the Discovery Rules tab button in the Discovery Manager form.

ii Click on the Apply button.

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 sets the device in a managed state and reconciles the device elements into its 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 the Managed State tab in the Discovery Manager form.

A list of managed devices appears.

The management state of the device is displayed in the Site State column. Managed is the default state. If the device is unmanaged, double click on the device and set the site state parameter to Managed in the form that appears.

- 5 From the Managed State tab, you can also perform management IP address pings to ensure connectivity to all the managed devices.

- i Click on one of the managed devices in the list.
- ii Click on the appropriate ping button.
 - Click on the Ping Out-of-Band button to test the management IP address, called an out-of-band management interface
 - Click on the Ping In-Band button to test the system IP address, called an in-band management interface
 - Click on the Ping Stby CPM button to test the IP address of the standby Control card, also called a CPM

The appropriate ping command is performed.

- iii Review the ping information to verify connectivity.

- 6 Verify that the device configuration has been reconciled into the 5620 SAM database by clicking the Resync Status tab button.

The status is displayed in the Resync Status column.

- Done indicates the database has been successfully reconciled.
- Failed indicates the database has not been successfully reconciled.

To initiate a manual reconciliation of a router, select the router from the router list and click 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 appears.
- Check your SNMP security parameters on a device using the CLI.
- Check your 5620 SAM poller policy settings by choosing Mediation→Poller Policies from the 5620 SAM main menu.

Devices that have been successfully reconciled appear in 5620 SAM navigation tree and the Equipment Manager form.

Procedure 6-4 To edit a discovery rule

Edit discovery rules:

- when new devices are added to the network
- when existing devices change system IDs

When you change system IDs, you must ensure that existing discovery rules are modified or the 5620 SAM considers the device with the modified system ID as a new device to be managed. Otherwise, the device you wanted to unmanaged continues to be polled by the discovery rules and re-discovered.

- Un-manage the device as described in Procedure 6-8
- Remove the device from any applicable discovery rules as described in this procedure
- Remove the management IP address of the device from any applicable discovery rules as described in this procedure
- Create or modify discovery rules to re-discover the device with the modified system ID
- Re-discover the device

- 1 Choose Mediation→Discovery Manager from the 5620 SAM main menu.

The Discovery Manager form appears.

- 2 Click on the Discovery Rules tab button.

- 3 Select a discovery rule from the list.

- 4 Click on the Edit button.

The appropriate TopologyDiscoveryRule edit form appears.

- 5 Configure the parameters, as required.

- i For example, to remove a rule element, click on the Rule Elements tab button

- ii Select the rule from the list.

- iii Click on the Remove button.

- 6 Click on the OK button to close the discovery rules editing form.

- 7 Perform steps 3 to 6 in Procedure 6-3.
-

Procedure 6-5 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 poller manager form. If you discovery rule is disabled, the network is not scanned as specified by these conditions.

- 1 Choose Mediation→Discovery Manager from the main menu.

The Discovery Manager form appears.

- 2 Click on the Discovery Rules tab button.

- 3 Select a discovery rule from the list.

- 4 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 6-6 To remove a discovery rule

When you remove a discovery rule, only the rule is removed. Discovered routers are not removed from the 5620 SAM.

- 1 Choose Mediation→Discovery Manager from the 5620 SAM main menu.

The Discovery Manager form appears.
 - 2 Click the Discovery Rules tab.
 - 3 Select a discovery rule from the list.
 - 4 Click the Remove button.
 - 5 Click the Apply button to delete the rule.
-

Procedure 6-7 To rescan the network

Perform this procedure to discover devices by rescanning the network as specified by a discovery rule.

- 1 Choose Mediation→Discovery Manager from the 5620 SAM main menu.

The Discovery Manager form appears.
- 2 Click on the Discovery Rules tab button.
- 3 Select one or more discovery rules from the list.
- 4 Click on the Rescan button.

The 5620 SAM scans the network as specified by the discovery rules and discovers devices. After a device is discovered, the 5620 SAM sets the device in a managed state and reconciles the device elements into its database.

- 5 Perform steps 4 and 6 in Procedure 6-3 to verify that the device has been successfully discovered and reconciled.
-

Procedure 6-8 To manage or unmanage a device

- 1 Choose Mediation→Discovery Manager from the main menu.

The Discovery Manager form appears.

- 2 Click on the Managed State tab button.
- 3 Select a device from the list.
- 4 Click on the Manage or Unmanage button as required
- 5 Verify the action.

The device becomes managed or unmanaged by the 5620 SAM.

Procedure 6-9 To reconcile device elements in the 5620 SAM database

Perform this procedure to reconcile device elements in the 5620 SAM database, for example, if the initial reconciliation failed.

- 1 Choose Mediation→Discovery Manager from the 5620 SAM main menu.
The Discovery Manager form appears.
- 2 Click on the Resync Status tab button.
- 3 Select a device from the list.
- 4 Click on the Resync button. The Resync Site form appears.
- 5 Choose a resynchronization option.
 - a Select the Resync All MIB Entries radio button to resync all MIBs for the router. Go to step 6.
 - b Select the Choose MIB Entries radio button resync some MIBs for the router. When you Select Choose MIB Entries, the Choose MIB Entries step appears.
 - i Click on the Next button
 - ii Choose one or more MIB entries from the list. Table 6-3 lists all the SNMP MIBs.
 - iii Click on the Next button.
- 6 The Force Resync form appears. Select the Ignore Timestamps check box to unconditionally resynchronize with the network device. When you do not select the Ignore Timestamps check box, MIBs are not resynchronized if the last change timestamp is unchanged.
- 7 Click on the Finish button.
- 8 A message indicates when the reconciliation is successful.

- 9 Perform step 6 in Procedure 6-3 to verify that the router elements have been reconciled in the 5620 SAM database.

6.6 SNMP MIBs

Poller policies define the interval and ratio used by 5620 SAM to poll network elements for MIB configuration changes. You can use the poller manager and poller policy forms to view the network element information contained in the MIB. See Procedure 6-1 for more information.

Table 6-3 lists the available polling options for MIBs and MIB entries.

Table 6-3 SNMP MIBs

Device name	MIB version	MIB name	MIB entry name
Alcatel-ESS-7450	1.0.0	EtherLike-MIB	dot3StatsEntry
Alcatel-ESS-7450	1.0.0	FRAME-RELAY-DTE-MIB	frDlcmiEntry
Alcatel-ESS-7450	1.0.0	HC-RMON-MIB	mediaIndependentEntry
Alcatel-ESS-7450	1.0.0	IEEE8023-LAG-MIB	dot3adAggEntry
Alcatel-ESS-7450	1.0.0		dot3adAggPortEntry
Alcatel-ESS-7450	1.0.0	IF-MIB	ifEntry
Alcatel-ESS-7450	1.0.0		ifXEntry
Alcatel-ESS-7450	1.0.0		linkDown
Alcatel-ESS-7450	1.0.0		linkUp
Alcatel-ESS-7450	1.0.0	IP-MIB	ipNetToMediaEntry
Alcatel-ESS-7450	1.0.0	ISIS-MIB	isisAreaAddrEntry
Alcatel-ESS-7450	1.0.0		isisCircEntry
Alcatel-ESS-7450	1.0.0		isisCircLevelEntry
Alcatel-ESS-7450	1.0.0		isisManAreaAddrEntry
Alcatel-ESS-7450	1.0.0		isisPacketCountEntry
Alcatel-ESS-7450	1.0.0		isisSysEntry
Alcatel-ESS-7450	1.0.0	MPLS-LSR-MIB	mplsInSegmentEntry
Alcatel-ESS-7450	1.0.0		mplsInterfaceConfEntry
Alcatel-ESS-7450	1.0.0		mplsOutSegmentEntry
Alcatel-ESS-7450	1.0.0		mplsXCDown
Alcatel-ESS-7450	1.0.0		mplsXCEntry
Alcatel-ESS-7450	1.0.0		mplsXCUp

(1 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-ESS-7450	1.0.0	MPLS-TE-MIB	mplsTunnelARHopEntry
Alcatel-ESS-7450	1.0.0		mplsTunnelDown
Alcatel-ESS-7450	1.0.0		mplsTunnelEntry
Alcatel-ESS-7450	1.0.0		mplsTunnelHopEntry
Alcatel-ESS-7450	1.0.0		mplsTunnelReoptimized
Alcatel-ESS-7450	1.0.0		mplsTunnelRerouted
Alcatel-ESS-7450	1.0.0		mplsTunnelUp
Alcatel-ESS-7450	1.0.0	OSPF-MIB	ospfASBdrRtrStatus
Alcatel-ESS-7450	1.0.0		ospfAdminStat
Alcatel-ESS-7450	1.0.0		ospfAreaAggregateEntry
Alcatel-ESS-7450	1.0.0		ospfAreaBdrRtrStatus
Alcatel-ESS-7450	1.0.0		ospfAreaEntry
Alcatel-ESS-7450	1.0.0		ospfExitOverflowInterval
Alcatel-ESS-7450	1.0.0		ospfExtLsdbLimit
Alcatel-ESS-7450	1.0.0		ospfExternLsaChecksumSum
Alcatel-ESS-7450	1.0.0		ospfExternLsaCount
Alcatel-ESS-7450	1.0.0		ospfIfEntry
Alcatel-ESS-7450	1.0.0		ospfIfMetricEntry
Alcatel-ESS-7450	1.0.0		ospfNbrEntry
Alcatel-ESS-7450	1.0.0		ospfOpaqueLsaSupport
Alcatel-ESS-7450	1.0.0		ospfRFC1583Compatibility
Alcatel-ESS-7450	1.0.0		ospfStubAreaEntry
Alcatel-ESS-7450	1.0.0		ospfTrafficEngineeringSupport
Alcatel-ESS-7450	1.0.0		ospfVirtIfEntry
Alcatel-ESS-7450	1.0.0	ospfVirtNbrEntry	

(2 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-ESS-7450	1.0.0	OSPF-TRAP-MIB	ospflfAuthFailure
Alcatel-ESS-7450	1.0.0		ospflfConfigError
Alcatel-ESS-7450	1.0.0		ospflfRxBadPacket
Alcatel-ESS-7450	1.0.0		ospflfStateChange
Alcatel-ESS-7450	1.0.0		ospfLsdbApproachingOverflow
Alcatel-ESS-7450	1.0.0		ospfLsdbOverflow
Alcatel-ESS-7450	1.0.0		ospfNbrStateChange
Alcatel-ESS-7450	1.0.0		ospfNssaTranslatorStatusChange
Alcatel-ESS-7450	1.0.0		ospfTxRetransmit
Alcatel-ESS-7450	1.0.0		ospfVirtIfAuthFailure
Alcatel-ESS-7450	1.0.0		ospfVirtIfConfigError
Alcatel-ESS-7450	1.0.0		ospfVirtIfRxBadPacket
Alcatel-ESS-7450	1.0.0		ospfVirtIfStateChange
Alcatel-ESS-7450	1.0.0		ospfVirtIfTxRetransmit
Alcatel-ESS-7450	1.0.0		ospfVirtNbrStateChange
Alcatel-ESS-7450	1.0.0	RSVP-MIB	rsvpIfEntry
Alcatel-ESS-7450	1.0.0		rsvpNbrEntry
Alcatel-ESS-7450	1.0.0	SNMP-USER-BASED-SM-MIB	usmUserEntry
Alcatel-ESS-7450	1.0.0	SNMP-VIEW-BASED-ACM-MIB	vacmAccessEntry
Alcatel-ESS-7450	1.0.0		vacmSecurityToGroupEntry
Alcatel-ESS-7450	1.0.0	SNMPv2-MIB	sysUpTime
Alcatel-ESS-7450	1.0.0	SONET-MIB	sonetFarEndLineCurrentEntry
Alcatel-ESS-7450	1.0.0		sonetFarEndLineIntervalEntry
Alcatel-ESS-7450	1.0.0		sonetFarEndPathCurrentEntry
Alcatel-ESS-7450	1.0.0		sonetFarEndPathIntervalEntry
Alcatel-ESS-7450	1.0.0		sonetLineCurrentEntry
Alcatel-ESS-7450	1.0.0		sonetLineIntervalEntry
Alcatel-ESS-7450	1.0.0		sonetPathCurrentEntry
Alcatel-ESS-7450	1.0.0		sonetPathIntervalEntry
Alcatel-ESS-7450	1.0.0		sonetSectionCurrentEntry
Alcatel-ESS-7450	1.0.0		sonetSectionIntervalEntry

(3 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-ESS-7450	1.0.0	TIMETRA-CHASSIS-MIB	tSyncIfTimingAdmEntry
Alcatel-ESS-7450	1.0.0		tmnxCardEntry
Alcatel-ESS-7450	1.0.0		tmnxChassisEntry
Alcatel-ESS-7450	1.0.0		tmnxChassisFanEntry
Alcatel-ESS-7450	1.0.0		tmnxChassisNotificationClear
Alcatel-ESS-7450	1.0.0		tmnxChassisPowerSupplyEntry
Alcatel-ESS-7450	1.0.0		tmnxCpmCardEntry
Alcatel-ESS-7450	1.0.0		tmnxCpmFlashEntry
Alcatel-ESS-7450	1.0.0		tmnxEnvTempTooHigh
Alcatel-ESS-7450	1.0.0		tmnxEqBackdoorBusFailure
Alcatel-ESS-7450	1.0.0		tmnxEqCardFailure
Alcatel-ESS-7450	1.0.0		tmnxEqCardInserted
Alcatel-ESS-7450	1.0.0		tmnxEqCardRemoved
Alcatel-ESS-7450	1.0.0		tmnxEqCpuFailure
Alcatel-ESS-7450	1.0.0		tmnxEqFanFailure
Alcatel-ESS-7450	1.0.0		tmnxEqFlashDataLoss
Alcatel-ESS-7450	1.0.0		tmnxEqFlashDiskFull
Alcatel-ESS-7450	1.0.0		tmnxEqMemoryFailure
Alcatel-ESS-7450	1.0.0		tmnxEqPowerSupplyFailure
Alcatel-ESS-7450	1.0.0		tmnxEqPowerSupplyInserted
Alcatel-ESS-7450	1.0.0		tmnxEqPowerSupplyRemoved
Alcatel-ESS-7450	1.0.0		tmnxEqWrongCard
Alcatel-ESS-7450	1.0.0		tmnxFabricEntry
Alcatel-ESS-7450	1.0.0		tmnxHwConfigChange
Alcatel-ESS-7450	1.0.0		tmnxHwEntry
Alcatel-ESS-7450	1.0.0		tmnxMDAEntry
Alcatel-ESS-7450	1.0.0		tmnxPeBootloaderVersionMismatch
Alcatel-ESS-7450	1.0.0		tmnxPeBootromVersionMismatch
Alcatel-ESS-7450	1.0.0		tmnxPeConfigurationError
Alcatel-ESS-7450	1.0.0		tmnxPeCpuCyclesExceeded
Alcatel-ESS-7450	1.0.0	tmnxPeFPGAVersionMismatch	

(4 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-ESS-7450	1.0.0	TIMETRA-CHASSIS-MIB continued	tmnxPeOutOfMemory
Alcatel-ESS-7450	1.0.0		tmnxPeSoftwareAbnormalHalt
Alcatel-ESS-7450	1.0.0		tmnxPeSoftwareError
Alcatel-ESS-7450	1.0.0		tmnxPeSoftwareLoadFailed
Alcatel-ESS-7450	1.0.0		tmnxPeSoftwareVersionMismatch
Alcatel-ESS-7450	1.0.0		tmnxPeStorageProblem
Alcatel-ESS-7450	1.0.0		tmnxRedPrimaryCPMFail
Alcatel-ESS-7450	1.0.0		tmnxRedRestoreFail
Alcatel-ESS-7450	1.0.0		tmnxRedRestoreSuccess
Alcatel-ESS-7450	1.0.0		tmnxRedSecondaryCPMStatusChange
Alcatel-ESS-7450	1.0.0		tmnxSynclfTimingEntry
Alcatel-ESS-7450	1.0.0	TIMETRA-FILTER-MIB	tIPFilterEntry
Alcatel-ESS-7450	1.0.0		tIPFilterParamsEntry
Alcatel-ESS-7450	1.0.0		tMacFilterEntry
Alcatel-ESS-7450	1.0.0		tMacFilterParamsEntry
Alcatel-ESS-7450	1.0.0	TIMETRA-ISIS-MIB	vRtrIisisAreaMismatch
Alcatel-ESS-7450	1.0.0		vRtrIisisAutTypeFail
Alcatel-ESS-7450	1.0.0		vRtrIisisAuthFail
Alcatel-ESS-7450	1.0.0		vRtrIisisEntry
Alcatel-ESS-7450	1.0.0		vRtrIisisIfEntry
Alcatel-ESS-7450	1.0.0		vRtrIisisIfLevelEntry
Alcatel-ESS-7450	1.0.0		vRtrIisisLevelEntry
Alcatel-ESS-7450	1.0.0		vRtrIisisManualAddressDrops
Alcatel-ESS-7450	1.0.0		vRtrIisisStatsEntry
Alcatel-ESS-7450	1.0.0	TIMETRA-LAG-MIB	tLagConfigEntry
Alcatel-ESS-7450	1.0.0		tLagDynamicCostOff
Alcatel-ESS-7450	1.0.0		tLagDynamicCostOn
Alcatel-ESS-7450	1.0.0		tLagOperationEntry
Alcatel-ESS-7450	1.0.0		tLagPortAddFailed

(5 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-ESS-7450	1.0.0	TIMETRA-LDP-MIB	vRtrLdpGeneralEntry
Alcatel-ESS-7450	1.0.0		vRtrLdpHelloAdjEntry
Alcatel-ESS-7450	1.0.0		vRtrLdpIfEntry
Alcatel-ESS-7450	1.0.0		vRtrLdpIfStateChange
Alcatel-ESS-7450	1.0.0		vRtrLdpIfStatsEntry
Alcatel-ESS-7450	1.0.0		vRtrLdpInstanceStateChange
Alcatel-ESS-7450	1.0.0		vRtrLdpPeerParamsEntry
Alcatel-ESS-7450	1.0.0		vRtrLdpSessionEntry
Alcatel-ESS-7450	1.0.0		vRtrLdpSessionStatsEntry
Alcatel-ESS-7450	1.0.0		vRtrLdpStateChange
Alcatel-ESS-7450	1.0.0		vRtrLdpStatsEntry
Alcatel-ESS-7450	1.0.0	TIMETRA-LOG-MIB	tmnxLogApEntry
Alcatel-ESS-7450	1.0.0		tmnxLogFileIdEntry
Alcatel-ESS-7450	1.0.0		tmnxLogFileRollover
Alcatel-ESS-7450	1.0.0	TIMETRA-MPLS-MIB	vRtrMplsAdminGroupEntry
Alcatel-ESS-7450	1.0.0		vRtrMplsGeneralEntry
Alcatel-ESS-7450	1.0.0		vRtrMplsGeneralStatEntry
Alcatel-ESS-7450	1.0.0		vRtrMplsIfEntry
Alcatel-ESS-7450	1.0.0		vRtrMplsIfStatEntry
Alcatel-ESS-7450	1.0.0		vRtrMplsIfStateChange
Alcatel-ESS-7450	1.0.0		vRtrMplsLspDown
Alcatel-ESS-7450	1.0.0		vRtrMplsLspEntry
Alcatel-ESS-7450	1.0.0		vRtrMplsLspPathDown
Alcatel-ESS-7450	1.0.0		vRtrMplsLspPathEntry
Alcatel-ESS-7450	1.0.0		vRtrMplsLspPathStatEntry
Alcatel-ESS-7450	1.0.0		vRtrMplsLspPathUp
Alcatel-ESS-7450	1.0.0		vRtrMplsLspStatEntry
Alcatel-ESS-7450	1.0.0		vRtrMplsLspUp
Alcatel-ESS-7450	1.0.0		vRtrMplsStateChange
Alcatel-ESS-7450	1.0.0		vRtrMplsTunnelCHopEntry
Alcatel-ESS-7450	1.0.0	vRtrMplsXCEntry	

(6 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-ESS-7450	1.0.0	TIMETRA-OAM-TEST-MIB	tmnxOamLspPingCtlEntry
Alcatel-ESS-7450	1.0.0		tmnxOamLspTrCtlEntry
Alcatel-ESS-7450	1.0.0		tmnxOamLspTrDSLLabelEntry
Alcatel-ESS-7450	1.0.0		tmnxOamLspTrMapEntry
Alcatel-ESS-7450	1.0.0		tmnxOamMacPingCtlEntry
Alcatel-ESS-7450	1.0.0		tmnxOamMacPingHistoryEntry
Alcatel-ESS-7450	1.0.0		tmnxOamMacTrCtlEntry
Alcatel-ESS-7450	1.0.0		tmnxOamMacTrL2MapEntry
Alcatel-ESS-7450	1.0.0		tmnxOamPingCtlEntry
Alcatel-ESS-7450	1.0.0		tmnxOamPingHistoryEntry
Alcatel-ESS-7450	1.0.0		tmnxOamPingProbeFailed
Alcatel-ESS-7450	1.0.0		tmnxOamPingResultsEntry
Alcatel-ESS-7450	1.0.0		tmnxOamPingTestCompleted
Alcatel-ESS-7450	1.0.0		tmnxOamPingTestFailed
Alcatel-ESS-7450	1.0.0		tmnxOamTrCtlEntry
Alcatel-ESS-7450	1.0.0		tmnxOamTrPathChange
Alcatel-ESS-7450	1.0.0		tmnxOamTrProbeHistoryEntry
Alcatel-ESS-7450	1.0.0		tmnxOamTrResultsEntry
Alcatel-ESS-7450	1.0.0		tmnxOamTrTestCompleted
Alcatel-ESS-7450	1.0.0		tmnxOamTrTestFailed

(7 of 30)

Device name	MIB version	MIB name	MIB entry name	
Alcatel-ESS-7450	1.0.0	TIMETRA-OSPF-MIB	vRtrOspfAreaEntry	
Alcatel-ESS-7450	1.0.0		vRtrOspfAvgSpfRunTime	
Alcatel-ESS-7450	1.0.0		vRtrOspfBackBoneRouter	
Alcatel-ESS-7450	1.0.0		vRtrOspfBaseRefCost	
Alcatel-ESS-7450	1.0.0		vRtrOspfExportPolicy1	
Alcatel-ESS-7450	1.0.0		vRtrOspfExportPolicy2	
Alcatel-ESS-7450	1.0.0		vRtrOspfExportPolicy3	
Alcatel-ESS-7450	1.0.0		vRtrOspfExportPolicy4	
Alcatel-ESS-7450	1.0.0		vRtrOspfExportPolicy5	
Alcatel-ESS-7450	1.0.0		vRtrOspfExtSpfRunTime	
Alcatel-ESS-7450	1.0.0		vRtrOspfExtSpfRuns	
Alcatel-ESS-7450	1.0.0		vRtrOspfExternalPreference	
Alcatel-ESS-7450	1.0.0		vRtrOspfIfEntry	
Alcatel-ESS-7450	1.0.0		vRtrOspfIfMD5KeyEntry	
Alcatel-ESS-7450	1.0.0		vRtrOspfInOverflowState	
Alcatel-ESS-7450	1.0.0		vRtrOspfIncrementalExtSpfRuns	
Alcatel-ESS-7450	1.0.0		vRtrOspfIncrementalInterSpfRuns	
Alcatel-ESS-7450	1.0.0		vRtrOspfLastEnabledTime	
Alcatel-ESS-7450	1.0.0		vRtrOspfLastExtSpfRunTime	
Alcatel-ESS-7450	1.0.0		vRtrOspfLastOverflowEnteredTime	
Alcatel-ESS-7450	1.0.0		vRtrOspfLastOverflowExitTime	
Alcatel-ESS-7450	1.0.0		vRtrOspfLsaAgingInterval	
Alcatel-ESS-7450	1.0.0		vRtrOspfMaxLsaAgingCount	
Alcatel-ESS-7450	1.0.0		vRtrOspfMaxSpfRunTime	
Alcatel-ESS-7450	1.0.0		vRtrOspfMinSpfRunTime	
Alcatel-ESS-7450	1.0.0		vRtrOspfNbrEntry	
Alcatel-ESS-7450	1.0.0		vRtrOspfPreference	
Alcatel-ESS-7450	1.0.0		vRtrOspfSpfHoldDown	
Alcatel-ESS-7450	1.0.0		vRtrOspfSpfSpacing	
Alcatel-ESS-7450	1.0.0		vRtrOspfTransmitInterval	
Alcatel-ESS-7450	1.0.0		vRtrOspfType11LsaChecksumSum	
Alcatel-ESS-7450	1.0.0		TIMETRA-OSPF-MIB continued	vRtrOspfType11LsaCount
Alcatel-ESS-7450	1.0.0			vRtrOspfVirtIfEntry
Alcatel-ESS-7450	1.0.0		vRtrOspfVirtIfMD5KeyEntry	
Alcatel-ESS-7450	1.0.0		vRtrOspfVirtNbrEntry	

(8 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-ESS-7450	1.0.0	TIMETRA-PORT-MIB	tmnxBundleEntry
Alcatel-ESS-7450	1.0.0		tmnxBundleMemberEntry
Alcatel-ESS-7450	1.0.0		tmnxEqOobPortFailure
Alcatel-ESS-7450	1.0.0		tmnxEqPortError
Alcatel-ESS-7450	1.0.0		tmnxEqPortFailure
Alcatel-ESS-7450	1.0.0		tmnxEqPortSFPCorrupted
Alcatel-ESS-7450	1.0.0		tmnxEqPortSFPInserted
Alcatel-ESS-7450	1.0.0		tmnxEqPortSFPRemoved
Alcatel-ESS-7450	1.0.0		tmnxEqPortSonetAlarm
Alcatel-ESS-7450	1.0.0		tmnxEqPortSonetAlarmClear
Alcatel-ESS-7450	1.0.0		tmnxEqPortSonetPathAlarm
Alcatel-ESS-7450	1.0.0		tmnxEqPortSonetPathAlarmClear
Alcatel-ESS-7450	1.0.0		tmnxEqPortWrongSFP
Alcatel-ESS-7450	1.0.0		tmnxFRDIcmiEntry
Alcatel-ESS-7450	1.0.0		tmnxPortEntry
Alcatel-ESS-7450	1.0.0		tmnxPortEtherEntry
Alcatel-ESS-7450	1.0.0		tmnxPortNotifyBerSdTca
Alcatel-ESS-7450	1.0.0		tmnxPortNotifyBerSfTca
Alcatel-ESS-7450	1.0.0		tmnxPortToChannelEntry
Alcatel-ESS-7450	1.0.0		tmnxQosPoolAppEntry
Alcatel-ESS-7450	1.0.0	tmnxQosServiceDegraded	
Alcatel-ESS-7450	1.0.0	tmnxSonetEntry	
Alcatel-ESS-7450	1.0.0	tmnxSonetPathEntry	
Alcatel-ESS-7450	1.0.0	TIMETRA-PPP-MIB	tmnxPppCpDown
Alcatel-ESS-7450	1.0.0		tmnxPppCpEntry
Alcatel-ESS-7450	1.0.0		tmnxPppCpUp
Alcatel-ESS-7450	1.0.0		tmnxPppEntry
Alcatel-ESS-7450	1.0.0		tmnxPppKeepaliveFailure
Alcatel-ESS-7450	1.0.0		tmnxPppLqmFailure
Alcatel-ESS-7450	1.0.0		tmnxPppNcpDown
Alcatel-ESS-7450	1.0.0		tmnxPppNcpUp

(9 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-ESS-7450	1.0.0	TIMETRA-QOS-MIB	tNetworkEgressFCEntry
Alcatel-ESS-7450	1.0.0		tNetworkIngressDSCPEEntry
Alcatel-ESS-7450	1.0.0		tNetworkIngressDot1pEntry
Alcatel-ESS-7450	1.0.0		tNetworkIngressLSPEXPEEntry
Alcatel-ESS-7450	1.0.0		tNetworkPolicyEntry
Alcatel-ESS-7450	1.0.0		tNetworkQueueEntry
Alcatel-ESS-7450	1.0.0		tNetworkQueueFCEntry
Alcatel-ESS-7450	1.0.0		tNetworkQueuePolicyEntry
Alcatel-ESS-7450	1.0.0		tSapEgressEntry
Alcatel-ESS-7450	1.0.0		tSapEgressFCEntry
Alcatel-ESS-7450	1.0.0		tSapEgressQueueEntry
Alcatel-ESS-7450	1.0.0		tSapIngressDSCPEEntry
Alcatel-ESS-7450	1.0.0		tSapIngressDot1pEntry
Alcatel-ESS-7450	1.0.0		tSapIngressEntry
Alcatel-ESS-7450	1.0.0		tSapIngressFCEntry
Alcatel-ESS-7450	1.0.0		tSapIngressIPCriteriaEntry
Alcatel-ESS-7450	1.0.0		tSapIngressMacCriteriaEntry
Alcatel-ESS-7450	1.0.0		tSapIngressPrecEntry
Alcatel-ESS-7450	1.0.0		tSapIngressQueueEntry
Alcatel-ESS-7450	1.0.0		tSchedulerPolicyEntry
Alcatel-ESS-7450	1.0.0	tSlopePolicyEntry	
Alcatel-ESS-7450	1.0.0	tVirtualSchedulerEntry	
Alcatel-ESS-7450	1.0.0	TIMETRA-RIP-MIB	vRtrRipAuthFailure
Alcatel-ESS-7450	1.0.0		vRtrRipAuthTypeMismatch
Alcatel-ESS-7450	1.0.0		vRtrRipGroupEntry
Alcatel-ESS-7450	1.0.0		vRtrRipIfEntry
Alcatel-ESS-7450	1.0.0		vRtrRipIfStatEntry
Alcatel-ESS-7450	1.0.0		vRtrRipInstanceEntry
Alcatel-ESS-7450	1.0.0		vRtrRipInstanceRestarted
Alcatel-ESS-7450	1.0.0		vRtrRipInstanceShuttingDown

(10 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-ESS-7450	1.0.0	TIMETRA-ROUTE-POLICY-MIB	tRPAdminPSAcceptActionParamsEntry
Alcatel-ESS-7450	1.0.0		tRPAdminPSDefaultActionParamsEntry
Alcatel-ESS-7450	1.0.0		tRPAdminPSFromCriteriaEntry
Alcatel-ESS-7450	1.0.0		tRPAdminPSPParamsEntry
Alcatel-ESS-7450	1.0.0		tRPAdminPSToCriteriaEntry
Alcatel-ESS-7450	1.0.0		tRPAdminPolicyStatementEntry
Alcatel-ESS-7450	1.0.0		tRPAdminPrefixListEntry
Alcatel-ESS-7450	1.0.0	TIMETRA-RSVP-MIB	vRtrRsvpGeneralEntry
Alcatel-ESS-7450	1.0.0		vRtrRsvplfEntry
Alcatel-ESS-7450	1.0.0		vRtrRsvplfNbrStateDown
Alcatel-ESS-7450	1.0.0		vRtrRsvplfNbrStateUp
Alcatel-ESS-7450	1.0.0		vRtrRsvplfStatEntry
Alcatel-ESS-7450	1.0.0		vRtrRsvplfStateChange
Alcatel-ESS-7450	1.0.0		vRtrRsvpSessionEntry
Alcatel-ESS-7450	1.0.0		vRtrRsvpSessionStatEntry
Alcatel-ESS-7450	1.0.0	vRtrRsvpStateChange	

(11 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-ESS-7450	1.0.0	TIMETRA-SECURITY-MIB	tmnxMafEntry
Alcatel-ESS-7450	1.0.0		tmnxMafMatchEntry
Alcatel-ESS-7450	1.0.0		tmnxPasswordAging
Alcatel-ESS-7450	1.0.0		tmnxPasswordAttemptsCount
Alcatel-ESS-7450	1.0.0		tmnxPasswordAttemptsLockoutPeriod
Alcatel-ESS-7450	1.0.0		tmnxPasswordAttemptsTime
Alcatel-ESS-7450	1.0.0		tmnxPasswordAuthenOrder1
Alcatel-ESS-7450	1.0.0		tmnxPasswordAuthenOrder2
Alcatel-ESS-7450	1.0.0		tmnxPasswordAuthenOrder3
Alcatel-ESS-7450	1.0.0		tmnxPasswordComplexity
Alcatel-ESS-7450	1.0.0		tmnxPasswordMinLength
Alcatel-ESS-7450	1.0.0		tmnxRadiusAccounting
Alcatel-ESS-7450	1.0.0		tmnxRadiusAdminStatus
Alcatel-ESS-7450	1.0.0		tmnxRadiusAuthorization
Alcatel-ESS-7450	1.0.0		tmnxRadiusPort
Alcatel-ESS-7450	1.0.0		tmnxRadiusRetryAttempts
Alcatel-ESS-7450	1.0.0		tmnxRadiusServerEntry
Alcatel-ESS-7450	1.0.0		tmnxRadiusSourceAddress
Alcatel-ESS-7450	1.0.0		tmnxRadiusTimeout
Alcatel-ESS-7450	1.0.0		tmnxTacPlusAccounting
Alcatel-ESS-7450	1.0.0		tmnxTacPlusAcctRecType
Alcatel-ESS-7450	1.0.0		tmnxTacPlusAdminStatus
Alcatel-ESS-7450	1.0.0		tmnxTacPlusAuthorization
Alcatel-ESS-7450	1.0.0		tmnxTacPlusServerEntry
Alcatel-ESS-7450	1.0.0		tmnxTacPlusSingleConnection
Alcatel-ESS-7450	1.0.0		tmnxTacPlusSourceAddress
Alcatel-ESS-7450	1.0.0		tmnxTacPlusTimeout
Alcatel-ESS-7450	1.0.0		tmnxUserEntry
Alcatel-ESS-7450	1.0.0	tmnxUserProfileEntry	
Alcatel-ESS-7450	1.0.0	tmnxUserProfileMatchEntry	

(12 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-ESS-7450	1.0.0	TIMETRA-SERV-MIB	bridgedTLS
Alcatel-ESS-7450	1.0.0		custCreated
Alcatel-ESS-7450	1.0.0		custDeleted
Alcatel-ESS-7450	1.0.0		custInfoEntry
Alcatel-ESS-7450	1.0.0		custMultSvcSiteCreated
Alcatel-ESS-7450	1.0.0		custMultSvcSiteDeleted
Alcatel-ESS-7450	1.0.0		custMultiServiceSiteEntry
Alcatel-ESS-7450	1.0.0		higherPriorityBridge
Alcatel-ESS-7450	1.0.0		iesIfCreated
Alcatel-ESS-7450	1.0.0		iesIfDeleted
Alcatel-ESS-7450	1.0.0		iesIfEntry
Alcatel-ESS-7450	1.0.0		iesIfStatusChanged
Alcatel-ESS-7450	1.0.0		newRootBridge
Alcatel-ESS-7450	1.0.0		newRootVcpState
Alcatel-ESS-7450	1.0.0		receivedTCN
Alcatel-ESS-7450	1.0.0		sapBaseInfoEntry
Alcatel-ESS-7450	1.0.0		sapCreated
Alcatel-ESS-7450	1.0.0		sapDeleted
Alcatel-ESS-7450	1.0.0		sapEncapDot1d
Alcatel-ESS-7450	1.0.0		sapEncapPVST
Alcatel-ESS-7450	1.0.0		sapStatusChanged
Alcatel-ESS-7450	1.0.0		sapTlsInfoEntry
Alcatel-ESS-7450	1.0.0		sdpBindCreated
Alcatel-ESS-7450	1.0.0		sdpBindDeleted
Alcatel-ESS-7450	1.0.0		sdpBindEntry
Alcatel-ESS-7450	1.0.0		sdpBindStatusChanged
Alcatel-ESS-7450	1.0.0		sdpCreated
Alcatel-ESS-7450	1.0.0		sdpDeleted
Alcatel-ESS-7450	1.0.0		sdpInfoEntry
Alcatel-ESS-7450	1.0.0		sdpStatusChanged
Alcatel-ESS-7450	1.0.0	svcBaseInfoEntry	

(13 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-ESS-7450	1.0.0	TIMETRA-SERV-MIB continued	svcCreated
Alcatel-ESS-7450	1.0.0		svcDeleted
Alcatel-ESS-7450	1.0.0		svcStatusChanged
Alcatel-ESS-7450	1.0.0		svcTlsInfoEntry
Alcatel-ESS-7450	1.0.0		tlsFdbInfoEntry
Alcatel-ESS-7450	1.0.0		topologyChangeSapMajorState
Alcatel-ESS-7450	1.0.0		topologyChangeSapState
Alcatel-ESS-7450	1.0.0		topologyChangeVcpState
Alcatel-ESS-7450	1.0.0		unacknowledgedTCN
Alcatel-ESS-7450	1.0.0	TIMETRA-SYSTEM-MIB	sbiBootConfig
Alcatel-ESS-7450	1.0.0		sbiBootSnmpd
Alcatel-ESS-7450	1.0.0		sbiConfigStatus
Alcatel-ESS-7450	1.0.0		sbiPersistStatus
Alcatel-ESS-7450	1.0.0		sbiStandbyIpAddr
Alcatel-ESS-7450	1.0.0		sgiCpuUsage
Alcatel-ESS-7450	1.0.0		sgiMemoryUsed
Alcatel-ESS-7450	1.0.0		ssiSaveConfigFailed
Alcatel-ESS-7450	1.0.0		ssiSaveConfigSucceeded
Alcatel-ESS-7450	1.0.0		ssiSyncBootEnvFailed
Alcatel-ESS-7450	1.0.0		ssiSyncBootEnvOK
Alcatel-ESS-7450	1.0.0		ssiSyncConfigFailed
Alcatel-ESS-7450	1.0.0		ssiSyncConfigOK
Alcatel-ESS-7450	1.0.0		ssiSyncStatus
Alcatel-ESS-7450	1.0.0		sysLACPSsystemPriority
Alcatel-ESS-7450	1.0.0		tmnxConfigCreate
Alcatel-ESS-7450	1.0.0		tmnxConfigDelete
Alcatel-ESS-7450	1.0.0		tmnxConfigModify
Alcatel-ESS-7450	1.0.0		tmnxStateChange
Alcatel-ESS-7450	1.0.0		tmnxTrapDropped
Alcatel-ESS-7450	1.0.0	TIMETRA-VRTR-MIB	vRtrConfEntry
Alcatel-ESS-7450	1.0.0		vRtrIfEntry
Alcatel-ESS-7450	1.0.0		vRtrIpAddrEntry
Alcatel-ESS-7450	1.0.0		vRtrStatEntry
Alcatel-ESS-7450	1.0.0		vRtrStaticRouteEntry
Alcatel-ESS-7450	1.0.0		vRtrSvcIpRangeEntry

(14 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-SR-7750	2.0.0	BGP4-MIB	bgpBackwardTransition
Alcatel-SR-7750	2.0.0		bgpEstablished
Alcatel-SR-7750	2.0.0		bgpPeerEntry
Alcatel-SR-7750	2.0.0	DS1-MIB	dsx1CurrentEntry
Alcatel-SR-7750	2.0.0		dsx1FarEndCurrentEntry
Alcatel-SR-7750	2.0.0		dsx1FarEndIntervalEntry
Alcatel-SR-7750	2.0.0		dsx1FarEndTotalEntry
Alcatel-SR-7750	2.0.0		dsx1IntervalEntry
Alcatel-SR-7750	2.0.0		dsx1TotalEntry
Alcatel-SR-7750	2.0.0		DS3-MIB
Alcatel-SR-7750	2.0.0	dsx3FarEndCurrentEntry	
Alcatel-SR-7750	2.0.0	dsx3FarEndIntervalEntry	
Alcatel-SR-7750	2.0.0	dsx3FarEndTotalEntry	
Alcatel-SR-7750	2.0.0	dsx3IntervalEntry	
Alcatel-SR-7750	2.0.0	dsx3TotalEntry	
Alcatel-SR-7750	2.0.0	EtherLike-MIB	dot3StatsEntry
Alcatel-SR-7750	2.0.0	FRAME-RELAY-DTE-MIB	frDlcmiEntry
Alcatel-SR-7750	2.0.0	HC-RMON-MIB	mediaIndependentEntry
Alcatel-SR-7750	2.0.0	IEEE8023-LAG-MIB	dot3adAggEntry
Alcatel-SR-7750	2.0.0		dot3adAggPortEntry
Alcatel-SR-7750	2.0.0	IF-MIB	ifEntry
Alcatel-SR-7750	2.0.0		ifXEntry
Alcatel-SR-7750	2.0.0		linkDown
Alcatel-SR-7750	2.0.0		linkUp
Alcatel-SR-7750	2.0.0	IP-MIB	ipNetToMediaEntry
Alcatel-SR-7750	2.0.0	ISIS-MIB	isisAreaAddrEntry
Alcatel-SR-7750	2.0.0		isisCircEntry
Alcatel-SR-7750	2.0.0		isisCircLevelEntry
Alcatel-SR-7750	2.0.0		isisManAreaAddrEntry
Alcatel-SR-7750	2.0.0		isisPacketCountEntry
Alcatel-SR-7750	2.0.0		isisSysEntry

(15 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-SR-7750	2.0.0	MPLS-LSR-MIB	mplsInSegmentEntry
Alcatel-SR-7750	2.0.0		mplsInterfaceConfEntry
Alcatel-SR-7750	2.0.0		mplsOutSegmentEntry
Alcatel-SR-7750	2.0.0		mplsXCDown
Alcatel-SR-7750	2.0.0		mplsXCEntry
Alcatel-SR-7750	2.0.0		mplsXCUp
Alcatel-SR-7750	2.0.0	MPLS-TE-MIB	mplsTunnelARHopEntry
Alcatel-SR-7750	2.0.0		mplsTunnelDown
Alcatel-SR-7750	2.0.0		mplsTunnelEntry
Alcatel-SR-7750	2.0.0		mplsTunnelHopEntry
Alcatel-SR-7750	2.0.0		mplsTunnelReoptimized
Alcatel-SR-7750	2.0.0		mplsTunnelRerouted
Alcatel-SR-7750	2.0.0		mplsTunnelUp
Alcatel-SR-7750	2.0.0	OSPF-MIB	ospfASBdrRtrStatus
Alcatel-SR-7750	2.0.0		ospfAdminStat
Alcatel-SR-7750	2.0.0		ospfAreaAggregateEntry
Alcatel-SR-7750	2.0.0		ospfAreaBdrRtrStatus
Alcatel-SR-7750	2.0.0		ospfAreaEntry
Alcatel-SR-7750	2.0.0		ospfExitOverflowInterval
Alcatel-SR-7750	2.0.0		ospfExtLsdbLimit
Alcatel-SR-7750	2.0.0		ospfExternLsaChecksumSum
Alcatel-SR-7750	2.0.0		ospfExternLsaCount
Alcatel-SR-7750	2.0.0		ospfIfEntry
Alcatel-SR-7750	2.0.0		ospfIfMetricEntry
Alcatel-SR-7750	2.0.0		ospfNbrEntry
Alcatel-SR-7750	2.0.0		ospfOpaqueLsaSupport
Alcatel-SR-7750	2.0.0		ospfRFC1583Compatibility
Alcatel-SR-7750	2.0.0		ospfStubAreaEntry
Alcatel-SR-7750	2.0.0		ospfTrafficEngineeringSupport
Alcatel-SR-7750	2.0.0		ospfVirtIfEntry
Alcatel-SR-7750	2.0.0	ospfVirtNbrEntry	

(16 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-SR-7750	2.0.0	OSPF-TRAP-MIB	ospflfAuthFailure
Alcatel-SR-7750	2.0.0		ospflfConfigError
Alcatel-SR-7750	2.0.0		ospflfRxBadPacket
Alcatel-SR-7750	2.0.0		ospflfStateChange
Alcatel-SR-7750	2.0.0		ospflsdbApproachingOverflow
Alcatel-SR-7750	2.0.0		ospflsdbOverflow
Alcatel-SR-7750	2.0.0		ospflNbrStateChange
Alcatel-SR-7750	2.0.0		ospflNssaTranslatorStatusChange
Alcatel-SR-7750	2.0.0		ospflTxRetransmit
Alcatel-SR-7750	2.0.0		ospflVirtlfAuthFailure
Alcatel-SR-7750	2.0.0		ospflVirtlfConfigError
Alcatel-SR-7750	2.0.0		ospflVirtlfRxBadPacket
Alcatel-SR-7750	2.0.0		ospflVirtlfStateChange
Alcatel-SR-7750	2.0.0		ospflVirtlfTxRetransmit
Alcatel-SR-7750	2.0.0		ospflVirtNbrStateChange
Alcatel-SR-7750	2.0.0	RSVP-MIB	rsvpIfEntry
Alcatel-SR-7750	2.0.0		rsvpNbrEntry
Alcatel-SR-7750	2.0.0	SNMP-USER-BASED-SM-MIB	usmUserEntry
Alcatel-SR-7750	2.0.0	SNMP-VIEW-BASED-ACM-MIB	vacmAccessEntry
Alcatel-SR-7750	2.0.0		vacmSecurityToGroupEntry
Alcatel-SR-7750	2.0.0	SNMPv2-MIB	sysUpTime
Alcatel-SR-7750	2.0.0	SONET-MIB	sonetFarEndLineCurrentEntry
Alcatel-SR-7750	2.0.0		sonetFarEndLineIntervalEntry
Alcatel-SR-7750	2.0.0		sonetFarEndPathCurrentEntry
Alcatel-SR-7750	2.0.0		sonetFarEndPathIntervalEntry
Alcatel-SR-7750	2.0.0		sonetLineCurrentEntry
Alcatel-SR-7750	2.0.0		sonetLineIntervalEntry
Alcatel-SR-7750	2.0.0		sonetPathCurrentEntry
Alcatel-SR-7750	2.0.0		sonetPathIntervalEntry
Alcatel-SR-7750	2.0.0		sonetSectionCurrentEntry
Alcatel-SR-7750	2.0.0		sonetSectionIntervalEntry

(17 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-SR-7750	2.0.0	TIMETRA-BGP-MIB	tBgpConfederationEntry
Alcatel-SR-7750	2.0.0		tBgpInstanceEntry
Alcatel-SR-7750	2.0.0		tBgpMaxPrefix100
Alcatel-SR-7750	2.0.0		tBgpMaxPrefix90
Alcatel-SR-7750	2.0.0		tBgpPeerEntry
Alcatel-SR-7750	2.0.0		tBgpPeerGroupEntry
Alcatel-SR-7750	2.0.0		tBgpPeerOperEntry

(18 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-SR-7750	2.0.0	TIMETRA-CHASSIS-MIB	tSynclfTimingAdmEntry
Alcatel-SR-7750	2.0.0		tmnxCardEntry
Alcatel-SR-7750	2.0.0		tmnxChassisEntry
Alcatel-SR-7750	2.0.0		tmnxChassisFanEntry
Alcatel-SR-7750	2.0.0		tmnxChassisNotificationClear
Alcatel-SR-7750	2.0.0		tmnxChassisPowerSupplyEntry
Alcatel-SR-7750	2.0.0		tmnxCpmCardEntry
Alcatel-SR-7750	2.0.0		tmnxCpmFlashEntry
Alcatel-SR-7750	2.0.0		tmnxEnvTempTooHigh
Alcatel-SR-7750	2.0.0		tmnxEqBackdoorBusFailure
Alcatel-SR-7750	2.0.0		tmnxEqCardFailure
Alcatel-SR-7750	2.0.0		tmnxEqCardInserted
Alcatel-SR-7750	2.0.0		tmnxEqCardRemoved
Alcatel-SR-7750	2.0.0		tmnxEqCpuFailure
Alcatel-SR-7750	2.0.0		tmnxEqFanFailure
Alcatel-SR-7750	2.0.0		tmnxEqFlashDataLoss
Alcatel-SR-7750	2.0.0		tmnxEqFlashDiskFull
Alcatel-SR-7750	2.0.0		tmnxEqMemoryFailure
Alcatel-SR-7750	2.0.0		tmnxEqPowerSupplyFailure
Alcatel-SR-7750	2.0.0		tmnxEqPowerSupplyInserted
Alcatel-SR-7750	2.0.0		tmnxEqPowerSupplyRemoved
Alcatel-SR-7750	2.0.0		tmnxEqWrongCard
Alcatel-SR-7750	2.0.0		tmnxFabricEntry
Alcatel-SR-7750	2.0.0		tmnxHwConfigChange
Alcatel-SR-7750	2.0.0		tmnxHwEntry
Alcatel-SR-7750	2.0.0		tmnxMDAEntry
Alcatel-SR-7750	2.0.0		tmnxPeBootloaderVersionMismatch
Alcatel-SR-7750	2.0.0		tmnxPeBootromVersionMismatch
Alcatel-SR-7750	2.0.0		tmnxPeConfigurationError
Alcatel-SR-7750	2.0.0		tmnxPeCpuCyclesExceeded
Alcatel-SR-7750	2.0.0	tmnxPeFPGAVersionMismatch	

(19 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-SR-7750	2.0.0	TIMETRA-CHASSIS-MIB continued	tmnxPeOutOfMemory
Alcatel-SR-7750	2.0.0		tmnxPeSoftwareAbnormalHalt
Alcatel-SR-7750	2.0.0		tmnxPeSoftwareError
Alcatel-SR-7750	2.0.0		tmnxPeSoftwareLoadFailed
Alcatel-SR-7750	2.0.0		tmnxPeSoftwareVersionMismatch
Alcatel-SR-7750	2.0.0		tmnxPeStorageProblem
Alcatel-SR-7750	2.0.0		tmnxRedPrimaryCPMFail
Alcatel-SR-7750	2.0.0		tmnxRedRestoreFail
Alcatel-SR-7750	2.0.0		tmnxRedRestoreSuccess
Alcatel-SR-7750	2.0.0		tmnxRedSecondaryCPMStatusChange
Alcatel-SR-7750	2.0.0		tmnxSynclfTimingEntry
Alcatel-SR-7750	2.0.0	TIMETRA-FILTER-MIB	tIPFilterEntry
Alcatel-SR-7750	2.0.0		tIPFilterParamsEntry
Alcatel-SR-7750	2.0.0		tMacFilterEntry
Alcatel-SR-7750	2.0.0		tMacFilterParamsEntry
Alcatel-SR-7750	2.0.0	TIMETRA-ISIS-MIB	vRtrIisisAreaMismatch
Alcatel-SR-7750	2.0.0		vRtrIisisAutTypeFail
Alcatel-SR-7750	2.0.0		vRtrIisisAuthFail
Alcatel-SR-7750	2.0.0		vRtrIisisEntry
Alcatel-SR-7750	2.0.0		vRtrIisisIfEntry
Alcatel-SR-7750	2.0.0		vRtrIisisIfLevelEntry
Alcatel-SR-7750	2.0.0		vRtrIisisLevelEntry
Alcatel-SR-7750	2.0.0		vRtrIisisManualAddressDrops
Alcatel-SR-7750	2.0.0		vRtrIisisStatsEntry
Alcatel-SR-7750	2.0.0	TIMETRA-LAG-MIB	tLagConfigEntry
Alcatel-SR-7750	2.0.0		tLagDynamicCostOff
Alcatel-SR-7750	2.0.0		tLagDynamicCostOn
Alcatel-SR-7750	2.0.0		tLagOperationEntry
Alcatel-SR-7750	2.0.0		tLagPortAddFailed

(20 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-SR-7750	2.0.0	TIMETRA-LDP-MIB	vRtrLdpGeneralEntry
Alcatel-SR-7750	2.0.0		vRtrLdpHelloAdjEntry
Alcatel-SR-7750	2.0.0		vRtrLdpIfEntry
Alcatel-SR-7750	2.0.0		vRtrLdpIfStateChange
Alcatel-SR-7750	2.0.0		vRtrLdpIfStatsEntry
Alcatel-SR-7750	2.0.0		vRtrLdpInstanceStateChange
Alcatel-SR-7750	2.0.0		vRtrLdpPeerParamsEntry
Alcatel-SR-7750	2.0.0		vRtrLdpSessionEntry
Alcatel-SR-7750	2.0.0		vRtrLdpSessionStatsEntry
Alcatel-SR-7750	2.0.0		vRtrLdpStateChange
Alcatel-SR-7750	2.0.0		vRtrLdpStatsEntry
Alcatel-SR-7750	2.0.0	TIMETRA-LOG-MIB	tmnxLogApEntry
Alcatel-SR-7750	2.0.0		tmnxLogFileIdEntry
Alcatel-SR-7750	2.0.0		tmnxLogFileRollover
Alcatel-SR-7750	2.0.0	TIMETRA-MPLS-MIB	vRtrMplsAdminGroupEntry
Alcatel-SR-7750	2.0.0		vRtrMplsGeneralEntry
Alcatel-SR-7750	2.0.0		vRtrMplsGeneralStatEntry
Alcatel-SR-7750	2.0.0		vRtrMplsIfEntry
Alcatel-SR-7750	2.0.0		vRtrMplsIfStatEntry
Alcatel-SR-7750	2.0.0		vRtrMplsIfStateChange
Alcatel-SR-7750	2.0.0		vRtrMplsLspDown
Alcatel-SR-7750	2.0.0		vRtrMplsLspEntry
Alcatel-SR-7750	2.0.0		vRtrMplsLspPathDown
Alcatel-SR-7750	2.0.0		vRtrMplsLspPathEntry
Alcatel-SR-7750	2.0.0		vRtrMplsLspPathStatEntry
Alcatel-SR-7750	2.0.0		vRtrMplsLspPathUp
Alcatel-SR-7750	2.0.0		vRtrMplsLspStatEntry
Alcatel-SR-7750	2.0.0		vRtrMplsLspUp
Alcatel-SR-7750	2.0.0		vRtrMplsStateChange
Alcatel-SR-7750	2.0.0		vRtrMplsTunnelCHopEntry
Alcatel-SR-7750	2.0.0		vRtrMplsXCEntry

(21 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-SR-7750	2.0.0	TIMETRA-OAM-TEST-MIB	tmnxOamLspPingCtlEntry
Alcatel-SR-7750	2.0.0		tmnxOamLspTrCtlEntry
Alcatel-SR-7750	2.0.0		tmnxOamLspTrDSLLabelEntry
Alcatel-SR-7750	2.0.0		tmnxOamLspTrMapEntry
Alcatel-SR-7750	2.0.0		tmnxOamMacPingCtlEntry
Alcatel-SR-7750	2.0.0		tmnxOamMacPingHistoryEntry
Alcatel-SR-7750	2.0.0		tmnxOamMacTrCtlEntry
Alcatel-SR-7750	2.0.0		tmnxOamMacTrL2MapEntry
Alcatel-SR-7750	2.0.0		tmnxOamPingCtlEntry
Alcatel-SR-7750	2.0.0		tmnxOamPingHistoryEntry
Alcatel-SR-7750	2.0.0		tmnxOamPingProbeFailed
Alcatel-SR-7750	2.0.0		tmnxOamPingResultsEntry
Alcatel-SR-7750	2.0.0		tmnxOamPingTestCompleted
Alcatel-SR-7750	2.0.0		tmnxOamPingTestFailed
Alcatel-SR-7750	2.0.0		tmnxOamTrCtlEntry
Alcatel-SR-7750	2.0.0		tmnxOamTrHopsEntry
Alcatel-SR-7750	2.0.0		tmnxOamTrPathChange
Alcatel-SR-7750	2.0.0		tmnxOamTrProbeHistoryEntry
Alcatel-SR-7750	2.0.0		tmnxOamTrResultsEntry
Alcatel-SR-7750	2.0.0		tmnxOamTrTestCompleted
Alcatel-SR-7750	2.0.0		tmnxOamTrTestFailed
Alcatel-SR-7750	2.0.0		tmnxOamVprnPingCtlEntry
Alcatel-SR-7750	2.0.0		tmnxOamVprnTrCtlEntry
Alcatel-SR-7750	2.0.0		tmnxOamVprnTrL3MapEntry
Alcatel-SR-7750	2.0.0		tmnxOamVprnTrNextHopEntry
Alcatel-SR-7750	2.0.0		tmnxOamVprnTrRTEntry

(22 of 30)

Device name	MIB version	MIB name	MIB entry name	
Alcatel-SR-7750	2.0.0	TIMETRA-OSPF-MIB	vRtrOspfAreaEntry	
Alcatel-SR-7750	2.0.0		vRtrOspfAvgSpfRunTime	
Alcatel-SR-7750	2.0.0		vRtrOspfBackBoneRouter	
Alcatel-SR-7750	2.0.0		vRtrOspfBaseRefCost	
Alcatel-SR-7750	2.0.0		vRtrOspfExportPolicy1	
Alcatel-SR-7750	2.0.0		vRtrOspfExportPolicy2	
Alcatel-SR-7750	2.0.0		vRtrOspfExportPolicy3	
Alcatel-SR-7750	2.0.0		vRtrOspfExportPolicy4	
Alcatel-SR-7750	2.0.0		vRtrOspfExportPolicy5	
Alcatel-SR-7750	2.0.0		vRtrOspfExtSpfRunTime	
Alcatel-SR-7750	2.0.0		vRtrOspfExtSpfRuns	
Alcatel-SR-7750	2.0.0		vRtrOspfExternalPreference	
Alcatel-SR-7750	2.0.0		vRtrOspfIfEntry	
Alcatel-SR-7750	2.0.0		vRtrOspfIfMD5KeyEntry	
Alcatel-SR-7750	2.0.0		vRtrOspfInOverflowState	
Alcatel-SR-7750	2.0.0		vRtrOspfIncrementalExtSpfRuns	
Alcatel-SR-7750	2.0.0		vRtrOspfIncrementalInterSpfRuns	
Alcatel-SR-7750	2.0.0		vRtrOspfLastEnabledTime	
Alcatel-SR-7750	2.0.0		vRtrOspfLastExtSpfRunTime	
Alcatel-SR-7750	2.0.0		vRtrOspfLastOverflowEnteredTime	
Alcatel-SR-7750	2.0.0		vRtrOspfLastOverflowExitTime	
Alcatel-SR-7750	2.0.0		vRtrOspfLsaAgingInterval	
Alcatel-SR-7750	2.0.0		vRtrOspfMaxLsaAgingCount	
Alcatel-SR-7750	2.0.0		vRtrOspfMaxSpfRunTime	
Alcatel-SR-7750	2.0.0		vRtrOspfMinSpfRunTime	
Alcatel-SR-7750	2.0.0		vRtrOspfNbrEntry	
Alcatel-SR-7750	2.0.0		vRtrOspfPreference	
Alcatel-SR-7750	2.0.0		vRtrOspfSpfHoldDown	
Alcatel-SR-7750	2.0.0		vRtrOspfSpfSpacing	
Alcatel-SR-7750	2.0.0		vRtrOspfTransmitInterval	
Alcatel-SR-7750	2.0.0		vRtrOspfType11LsaChecksumSum	
Alcatel-SR-7750	2.0.0		TIMETRA-OSPF-MIB continued	vRtrOspfType11LsaCount
Alcatel-SR-7750	2.0.0			vRtrOspfVirtIfEntry
Alcatel-SR-7750	2.0.0		vRtrOspfVirtIfMD5KeyEntry	
Alcatel-SR-7750	2.0.0		vRtrOspfVirtNbrEntry	

(23 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-SR-7750	2.0.0	TIMETRA-PORT-MIB	tmnxBundleEntry
Alcatel-SR-7750	2.0.0		tmnxBundleMemberEntry
Alcatel-SR-7750	2.0.0		tmnxDS0ChanGroupEntry
Alcatel-SR-7750	2.0.0		tmnxDS1Entry
Alcatel-SR-7750	2.0.0		tmnxDS3ChannelEntry
Alcatel-SR-7750	2.0.0		tmnxDS3Entry
Alcatel-SR-7750	2.0.0		tmnxEqOobPortFailure
Alcatel-SR-7750	2.0.0		tmnxEqPortDS1Alarm
Alcatel-SR-7750	2.0.0		tmnxEqPortDS1AlarmClear
Alcatel-SR-7750	2.0.0		tmnxEqPortDS3Alarm
Alcatel-SR-7750	2.0.0		tmnxEqPortDS3AlarmClear
Alcatel-SR-7750	2.0.0		tmnxEqPortError
Alcatel-SR-7750	2.0.0		tmnxEqPortFailure
Alcatel-SR-7750	2.0.0		tmnxEqPortSFPCorrupted
Alcatel-SR-7750	2.0.0		tmnxEqPortSFPIinserted
Alcatel-SR-7750	2.0.0		tmnxEqPortSFPRemoved
Alcatel-SR-7750	2.0.0		tmnxEqPortSonetAlarm
Alcatel-SR-7750	2.0.0		tmnxEqPortSonetAlarmClear
Alcatel-SR-7750	2.0.0		tmnxEqPortSonetPathAlarm
Alcatel-SR-7750	2.0.0		tmnxEqPortSonetPathAlarmClear
Alcatel-SR-7750	2.0.0		tmnxEqPortWrongSFP
Alcatel-SR-7750	2.0.0		tmnxFRDlcmiEntry
Alcatel-SR-7750	2.0.0		tmnxPortEntry
Alcatel-SR-7750	2.0.0		tmnxPortEtherEntry
Alcatel-SR-7750	2.0.0		tmnxPortNotifyBerSdTca
Alcatel-SR-7750	2.0.0		tmnxPortNotifyBerSfTca
Alcatel-SR-7750	2.0.0		tmnxPortToChannelEntry
Alcatel-SR-7750	2.0.0		tmnxQosPoolAppEntry
Alcatel-SR-7750	2.0.0		tmnxQosServiceDegraded
Alcatel-SR-7750	2.0.0		tmnxSonetEntry
Alcatel-SR-7750	2.0.0	tmnxSonetPathEntry	

(24 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-SR-7750	2.0.0	TIMETRA-PPP-MIB	tmnxPppCpDown
Alcatel-SR-7750	2.0.0		tmnxPppCpEntry
Alcatel-SR-7750	2.0.0		tmnxPppCpUp
Alcatel-SR-7750	2.0.0		tmnxPppEntry
Alcatel-SR-7750	2.0.0		tmnxPppKeepaliveFailure
Alcatel-SR-7750	2.0.0		tmnxPppLqmFailure
Alcatel-SR-7750	2.0.0		tmnxPppNcpDown
Alcatel-SR-7750	2.0.0		tmnxPppNcpUp
Alcatel-SR-7750	2.0.0	TIMETRA-QOS-MIB	tNetworkEgressFCEntry
Alcatel-SR-7750	2.0.0		tNetworkIngressDSCPEEntry
Alcatel-SR-7750	2.0.0		tNetworkIngressDot1pEntry
Alcatel-SR-7750	2.0.0		tNetworkIngressLSPEXPEEntry
Alcatel-SR-7750	2.0.0		tNetworkPolicyEntry
Alcatel-SR-7750	2.0.0		tNetworkQueueEntry
Alcatel-SR-7750	2.0.0		tNetworkQueueFCEntry
Alcatel-SR-7750	2.0.0		tNetworkQueuePolicyEntry
Alcatel-SR-7750	2.0.0		tSapEgressEntry
Alcatel-SR-7750	2.0.0		tSapEgressFCEntry
Alcatel-SR-7750	2.0.0		tSapEgressQueueEntry
Alcatel-SR-7750	2.0.0		tSapIngressDSCPEEntry
Alcatel-SR-7750	2.0.0		tSapIngressDot1pEntry
Alcatel-SR-7750	2.0.0		tSapIngressEntry
Alcatel-SR-7750	2.0.0		tSapIngressFCEntry
Alcatel-SR-7750	2.0.0		tSapIngressIPCriteriasEntry
Alcatel-SR-7750	2.0.0		tSapIngressMacCriteriaEntry
Alcatel-SR-7750	2.0.0		tSapIngressPrecEntry
Alcatel-SR-7750	2.0.0		tSapIngressQueueEntry
Alcatel-SR-7750	2.0.0		tSchedulerPolicyEntry
Alcatel-SR-7750	2.0.0	tSlopePolicyEntry	
Alcatel-SR-7750	2.0.0	tVirtualSchedulerEntry	

(25 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-SR-7750	2.0.0	TIMETRA-RIP-MIB	vRtrRipAuthFailure
Alcatel-SR-7750	2.0.0		vRtrRipAuthTypeMismatch
Alcatel-SR-7750	2.0.0		vRtrRipGroupEntry
Alcatel-SR-7750	2.0.0		vRtrRipIfEntry
Alcatel-SR-7750	2.0.0		vRtrRipIfStatEntry
Alcatel-SR-7750	2.0.0		vRtrRipInstanceEntry
Alcatel-SR-7750	2.0.0		vRtrRipInstanceRestarted
Alcatel-SR-7750	2.0.0		vRtrRipInstanceShuttingDown
Alcatel-SR-7750	2.0.0	TIMETRA-ROUTE-POLICY-MIB	tRPAAdminASPathEntry
Alcatel-SR-7750	2.0.0		tRPAAdminCommunityEntry
Alcatel-SR-7750	2.0.0		tRPAAdminDampingEntry
Alcatel-SR-7750	2.0.0		tRPAAdminPSAcceptActionParamsEntry
Alcatel-SR-7750	2.0.0		tRPAAdminPSDefaultActionParamsEntry
Alcatel-SR-7750	2.0.0		tRPAAdminPSFromCriteriaEntry
Alcatel-SR-7750	2.0.0		tRPAAdminPSParamsEntry
Alcatel-SR-7750	2.0.0		tRPAAdminPSToCriteriaEntry
Alcatel-SR-7750	2.0.0		tRPAAdminPolicyStatementEntry
Alcatel-SR-7750	2.0.0		tRPAAdminPrefixListEntry
Alcatel-SR-7750	2.0.0	TIMETRA-RSVP-MIB	vRtrRsvpGeneralEntry
Alcatel-SR-7750	2.0.0		vRtrRsvpIfEntry
Alcatel-SR-7750	2.0.0		vRtrRsvpIfNbrStateDown
Alcatel-SR-7750	2.0.0		vRtrRsvpIfNbrStateUp
Alcatel-SR-7750	2.0.0		vRtrRsvpIfStatEntry
Alcatel-SR-7750	2.0.0		vRtrRsvpIfStateChange
Alcatel-SR-7750	2.0.0		vRtrRsvpSessionEntry
Alcatel-SR-7750	2.0.0		vRtrRsvpSessionStatEntry
Alcatel-SR-7750	2.0.0	vRtrRsvpStateChange	

(26 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-SR-7750	2.0.0	TIMETRA-SECURITY-MIB	tmnxMafEntry
Alcatel-SR-7750	2.0.0		tmnxMafMatchEntry
Alcatel-SR-7750	2.0.0		tmnxPasswordAging
Alcatel-SR-7750	2.0.0		tmnxPasswordAttemptsCount
Alcatel-SR-7750	2.0.0		tmnxPasswordAttemptsLockoutPeriod
Alcatel-SR-7750	2.0.0		tmnxPasswordAttemptsTime
Alcatel-SR-7750	2.0.0		tmnxPasswordAuthenOrder1
Alcatel-SR-7750	2.0.0		tmnxPasswordAuthenOrder2
Alcatel-SR-7750	2.0.0		tmnxPasswordAuthenOrder3
Alcatel-SR-7750	2.0.0		tmnxPasswordComplexity
Alcatel-SR-7750	2.0.0		tmnxPasswordMinLength
Alcatel-SR-7750	2.0.0		tmnxRadiusAccounting
Alcatel-SR-7750	2.0.0		tmnxRadiusAdminStatus
Alcatel-SR-7750	2.0.0		tmnxRadiusAuthorization
Alcatel-SR-7750	2.0.0		tmnxRadiusPort
Alcatel-SR-7750	2.0.0		tmnxRadiusRetryAttempts
Alcatel-SR-7750	2.0.0		tmnxRadiusServerEntry
Alcatel-SR-7750	2.0.0		tmnxRadiusSourceAddress
Alcatel-SR-7750	2.0.0		tmnxRadiusTimeout
Alcatel-SR-7750	2.0.0		tmnxTacPlusAccounting
Alcatel-SR-7750	2.0.0		tmnxTacPlusAcctRecType
Alcatel-SR-7750	2.0.0		tmnxTacPlusAdminStatus
Alcatel-SR-7750	2.0.0		tmnxTacPlusAuthorization
Alcatel-SR-7750	2.0.0		tmnxTacPlusServerEntry
Alcatel-SR-7750	2.0.0		tmnxTacPlusSingleConnection
Alcatel-SR-7750	2.0.0		tmnxTacPlusSourceAddress
Alcatel-SR-7750	2.0.0		tmnxTacPlusTimeout
Alcatel-SR-7750	2.0.0	tmnxUserEntry	
Alcatel-SR-7750	2.0.0	tmnxUserProfileEntry	
Alcatel-SR-7750	2.0.0	tmnxUserProfileMatchEntry	

(27 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-SR-7750	2.0.0	TIMETRA-SERV-MIB	bridgedTLS
Alcatel-SR-7750	2.0.0		custCreated
Alcatel-SR-7750	2.0.0		custDeleted
Alcatel-SR-7750	2.0.0		custInfoEntry
Alcatel-SR-7750	2.0.0		custMultSvcSiteCreated
Alcatel-SR-7750	2.0.0		custMultSvcSiteDeleted
Alcatel-SR-7750	2.0.0		custMultiServiceSiteEntry
Alcatel-SR-7750	2.0.0		higherPriorityBridge
Alcatel-SR-7750	2.0.0		iesIfCreated
Alcatel-SR-7750	2.0.0		iesIfDeleted
Alcatel-SR-7750	2.0.0		iesIfEntry
Alcatel-SR-7750	2.0.0		iesIfStatusChanged
Alcatel-SR-7750	2.0.0		newRootBridge
Alcatel-SR-7750	2.0.0		newRootSap
Alcatel-SR-7750	2.0.0		newRootVcpState
Alcatel-SR-7750	2.0.0		receivedTCN
Alcatel-SR-7750	2.0.0		sapBaselInfoEntry
Alcatel-SR-7750	2.0.0		sapCreated
Alcatel-SR-7750	2.0.0		sapDeleted
Alcatel-SR-7750	2.0.0		sapEncapDot1d
Alcatel-SR-7750	2.0.0		sapEncapPVST
Alcatel-SR-7750	2.0.0		sapStatusChanged
Alcatel-SR-7750	2.0.0		sapTlsInfoEntry
Alcatel-SR-7750	2.0.0		sdpBindCreated
Alcatel-SR-7750	2.0.0		sdpBindDeleted
Alcatel-SR-7750	2.0.0		sdpBindEntry
Alcatel-SR-7750	2.0.0		sdpBindStatusChanged
Alcatel-SR-7750	2.0.0		sdpCreated
Alcatel-SR-7750	2.0.0		sdpDeleted
Alcatel-SR-7750	2.0.0		sdpInfoEntry
Alcatel-SR-7750	2.0.0	sdpStatusChanged	

(28 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-SR-7750	2.0.0	TIMETRA-SERV-MIB continued	svcBaseInfoEntry
Alcatel-SR-7750	2.0.0		svcCreated
Alcatel-SR-7750	2.0.0		svcDeleted
Alcatel-SR-7750	2.0.0		svcStatusChanged
Alcatel-SR-7750	2.0.0		svcTlsInfoEntry
Alcatel-SR-7750	2.0.0		tlsFdbInfoEntry
Alcatel-SR-7750	2.0.0		topologyChangeSapMajorState
Alcatel-SR-7750	2.0.0		topologyChangeSapState
Alcatel-SR-7750	2.0.0		topologyChangeVcpState
Alcatel-SR-7750	2.0.0		unacknowledgedTCN
Alcatel-SR-7750	2.0.0		TIMETRA-SYSTEM-MIB
Alcatel-SR-7750	2.0.0	sbiBootSnmpd	
Alcatel-SR-7750	2.0.0	sbiConfigStatus	
Alcatel-SR-7750	2.0.0	sbiPersistStatus	
Alcatel-SR-7750	2.0.0	sbiStandbyIpAddr	
Alcatel-SR-7750	2.0.0	sgiCpuUsage	
Alcatel-SR-7750	2.0.0	sgiMemoryUsed	
Alcatel-SR-7750	2.0.0	ssiSaveConfigFailed	
Alcatel-SR-7750	2.0.0	ssiSaveConfigSucceeded	
Alcatel-SR-7750	2.0.0	ssiSyncBootEnvFailed	
Alcatel-SR-7750	2.0.0	ssiSyncBootEnvOK	
Alcatel-SR-7750	2.0.0	ssiSyncConfigFailed	
Alcatel-SR-7750	2.0.0	ssiSyncConfigOK	
Alcatel-SR-7750	2.0.0	ssiSyncStatus	
Alcatel-SR-7750	2.0.0	sysLACPSysPriority	
Alcatel-SR-7750	2.0.0	tmnxConfigCreate	
Alcatel-SR-7750	2.0.0	tmnxConfigDelete	
Alcatel-SR-7750	2.0.0	tmnxConfigModify	
Alcatel-SR-7750	2.0.0	tmnxStateChange	
Alcatel-SR-7750	2.0.0	tmnxTrapDropped	

(29 of 30)

Device name	MIB version	MIB name	MIB entry name
Alcatel-SR-7750	2.0.0	TIMETRA-VRTR-MIB	vRtrConfEntry
Alcatel-SR-7750	2.0.0		vRtrIfEntry
Alcatel-SR-7750	2.0.0		vRtrIpAddrEntry
Alcatel-SR-7750	2.0.0		vRtrPolicyEntry
Alcatel-SR-7750	2.0.0		vRtrStatEntry
Alcatel-SR-7750	2.0.0		vRtrStaticRouteEntry
Alcatel-SR-7750	2.0.0		vRtrSvcIplRangeEntry

(30 of 30)

7 — In-band and out-of-band management

- 7.1 Network element in-band and out-of-band management overview 7-2**
- 7.2 In-band and out-of-band management workflow 7-3**
- 7.3 In-band and out-of-band management menu 7-4**
- 7.4 In-band and out-of-band management procedure list 7-4**
- 7.5 In-band and out-of-band management procedure 7-4**

7.1 Network element in-band and out-of-band management overview

There are two ways for the 5620 SAM to send management traffic to the managed network:

- in-band using an Ethernet connection to the management interface of a device
- out-of-band using connectivity between devices

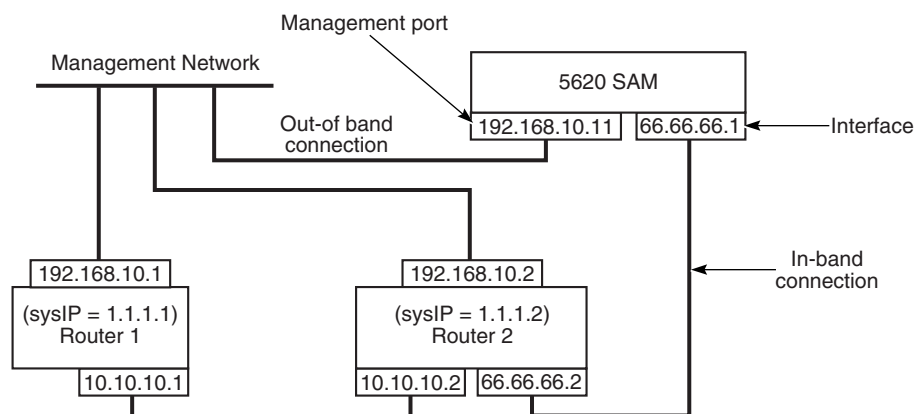
When you set up both types of management, network elements can be managed using alternate routes if a link fails.

In-band management, called secondary on the GUI, uses a connection provided by a customer service, such as a VLL. The management traffic is sent in-band along with the customer payload traffic. The packets with the management data arrive at the device using one of the interfaces. The destination address is the system IP address of the device. In-band management is typically used when the geography of dispersed sites makes it economically impractical to have out-of-band links. As well, an in-band connection can be configured as a safety measure, in case the primary out-of-band connection fails.

Out-of-band management, called primary on the GUI, uses a management connection to the management port of the device. The management traffic is sent out-of-band. The packets with the management data arrive at the device using the management port. The destination address is the management IP address of the device.

Figure 7-1 shows an example of in-band and out-of-band functionality.

Figure 7-1 Example of in-band and out-of-band traffic



17266

In this example, there needs to be a route that allows a ping from the 5620 SAM to the system IP address of router 1 (1.1.1.1).

Figure 7-2 shows the form to configure in-band and out-of-band management using the 5620 SAM GUI.

Figure 7-2 Network element form - Polling

7.2 In-band and out-of-band management workflow

- 1 Using the CLI, configure the SNMP security parameters on the devices that you want to discover.
- 2 Install and configure network interface cards on the 5620 SAM: one for in-band and one for out-of-band networks.
- 3 Configure each device for in-band and out-of-band management. In-band management used the system (loopback) address of the device. Out-of-band management uses a network port of the device.



Note — You must discover devices using an out-of-band connection.

- 4 Configure a second trap destination log on the device to ensure the 5620 SAM receives SNMP traps in-band. On the device type:

```
configure log log-id log_ID_number from main security
```

```
configure log log-id log_ID_number to snmp snmp_port_number
```

```
configure log snmp-trap-group snmp_trap_group_number
trap-destination ip_address "version_of_snmp" notify-community
" name_of_community "
```

- 5 Configure a route for in-band traffic. For example, a static route or by OSPF learning through being a neighbor.
- 6 Configure in-band or out-of band polling policies.

7.3 In-band and out-of-band management menu

Use the Equipment or Network tabs in the navigation tree, and select the icon representing the managed device.

7.4 In-band and out-of-band management procedure list

Table 7-1 lists the in-band and out-of-band management polling procedure.

Table 7-1 5620 SAM in-band and out-of-band procedure list

Procedure	Purpose
To configure in-band or out-of-band polling policies	To configure the 5620 SAM to use in-band, out-of-band, or both in-band and out-of-band management functionality.

7.5 In-band and out-of-band management procedure

This section provides the in-band and out-of-band management procedure.

Procedure 7-1 To configure in-band or out-of-band polling policies

Perform this procedure to configure the 5620 SAM to use in-band, out-of-band, or in-band and out-of-band polling in the intervals specified in the poller policies configuration, as described in chapter 6.

- 1 Click on the Equipment or Network tab button in the navigation tree.
- 2 Open the Network icon.
The managed devices are displayed.
- 3 Click on one or more icons that represent managed devices.
- 4 Right-click and choose Properties from the contextual menu.
The Network Element form appears.
- 5 Click on the Polling tab button.

6 Configure the parameters:

- i** Specify whether scheduled polling is enabled or disabled using the Scheduled Polling parameter. Scheduled polling is configured using the poller policies configuration form. See Procedure 6-1 in chapter 6 for more information.
- ii** Set the Active Management IP parameter. By default this is set to primary. The parameter specifies the currently used management method. Primary is the same as out-of-band. Secondary is the same as in-band.

You can change the management method by changing the Active Management IP parameter.

- iii** Check the Auto Revert to Primary check box to ensure that primary (out-of-band) management is used after a failed switch to secondary (in-band) management.
- iv** Specify whether to use Primary Only, Secondary Only, or Primary and Secondary as the management method using the Management IP Selection parameter.

When you choose Primary and Secondary, you can use the other parameters to control and regulate the management switch-over process.

7 Click on the Apply button to save the changes.

8 — Security management for 5620 SAM groups and users

- 8.1 Security management for 5620 SAM groups and users overview 8-2**
- 8.2 Workflow to manage security for 5620 SAM groups and users 8-4**
- 8.3 5620 SAM groups and users configuration procedures list 8-4**
- 8.4 5620 SAM groups and user configuration procedures 8-5**

8.1 Security management for 5620 SAM groups and users overview

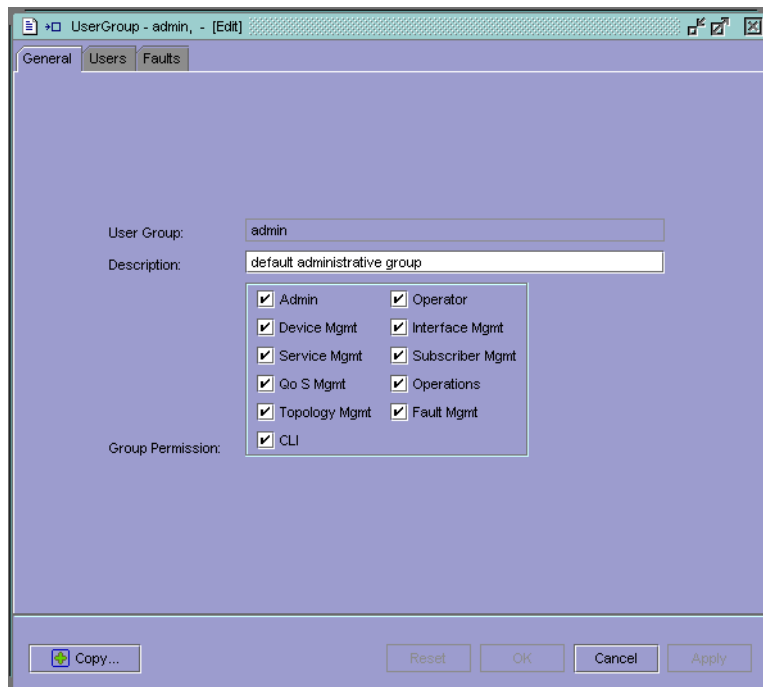
The system administrator uses security management forms to control group and user privileges on the 5620 SAM. Users are assigned to a group that has been configured with permissions for one or more functional areas of the 5620 SAM.

The system administrator can perform the following tasks:

- create groups and configure group permissions
- create users and assign users to groups
- modify users and groups
- modify user passwords
- suspend and re-instate users

Figure 8-1 shows an User Group security management form with the General tab chosen.

Figure 8-1 User Group security management form - General



The screenshot shows a window titled "UserGroup - admin, - [Edit]" with three tabs: "General", "Users", and "Faults". The "General" tab is selected. The form contains the following fields and options:

- User Group: admin
- Description: default administrative group
- Group Permission: A list of permissions with checkboxes, all of which are checked:
 - Admin
 - Device Mgmt
 - Service Mgmt
 - Go S Mgmt
 - Topology Mgmt
 - CLI
 - Operator
 - Interface Mgmt
 - Subscriber Mgmt
 - Operations
 - Fault Mgmt

At the bottom of the form, there are buttons for "Copy...", "Reset", "OK", "Cancel", and "Apply".

Figure 8-2 shows a User admin security management form with the General tab chosen.

Figure 8-2 User admin security management form for admin user - General

The screenshot shows a web-based form for editing user security settings. The title bar reads "User - admin, - securityManager:userGroup-admin [Edit]". The "General" tab is active. Fields include:

- User Name: admin
- Security Group: admin (with "Select..." and "View..." buttons)
- User State: resumed (dropdown menu)
- Digest: N/A
- Selected Group Permission: A list of permissions with checkboxes:
 - Admin (checked)
 - Operator (checked)
 - Device Mgmt (checked)
 - Interface Mgmt (checked)
 - Service Mgmt (checked)
 - Subscriber Mgmt (checked)
 - QoS Mgmt (checked)
 - Operations (checked)
 - Topology Mgmt (checked)
 - Fault Mgmt (checked)
 - CLI (checked)
- User Password: (empty field)
- Confirm Password: (empty field)

 At the bottom, there are buttons for "Copy...", "Reset", "OK", "Cancel", and "Apply".

Users and group permissions

Users have write access to 5620 SAM functional areas based on the group permissions for the group to which they belong.



Note — The term user applies to personnel who require system access to perform tasks. The term user does not apply to a subscriber.

The following general rules apply to users and groups:

- A user cannot belong to more than one group.
- Groups can be configured to allow access to one or more functional areas.
- All users can choose all 5620 SAM main menu options except the Security→Manage Security menu option.
- Only users with the appropriate permissions can configure parameters in the forms that appear when a main menu option is chosen.
- All users can view faults and alarms, but only users with access to the Fault Manager can manage alarms.
- All users have access to the topology views but only users with access to the Topology Manager can perform topology tasks.

Table 8-1 describes the group permissions.

Table 8-1 Group permissions

Permission group	Functional area access	Use to
Admin	All 5620 SAM functional areas	Perform all 5620 SAM tasks, including administering users and groups.
Device Mgmt	Equipment management	Configure and manage equipment operations and inventory.
Interface Mgmt	Interface management	Configure interface properties.
Topology Mgmt	Topology management	Monitor and manage network elements.
Subscriber Mgmt	Subscriber management	Configure and manage subscriber accounts.
Service Mgmt	Service management	Configure and manage service distribution paths and services.
QoS Mgmt	QoS policies	Configure and manage QoS and filter policies, counters, and manage DSCP and FC resources.
Fault Mgmt	Fault policies	Monitor and manage outstanding alarms, acknowledge and perform severity alterations, manage the alarm history database, and modify fault policies.
Operator	Read-only access to all functional areas, except the Security Manager	Monitor applications and faults.
Operations	System maintenance	Perform system maintenance functions such as managing logs, database backups and restores, and software downloads, adding and removing network nodes, and specifying mediation policies.
CLI	CLI	Start a CLI session from the chosen network element.

8.2 Workflow to manage security for 5620 SAM groups and users

- 1 Create groups of users according to types of tasks performed.
- 2 Create users that will perform the kind of tasks assigned to that group.
- 3 Manage groups.
 - modify groups
 - delete groups
- 4 Manage users.
 - modify users
 - delete users
 - suspend or re-instate users
 - change user passwords as system administrator
- 5 Change user password as user.

8.3 5620 SAM groups and users configuration procedures list

Table 8-2 lists the procedures necessary to create and manage groups and users.

Table 8-2 5620 SAM group and user procedures reference

Procedure	Purpose
To create 5620 SAM user groups	To create a group of users that have common privileges.
To create 5620 SAM user accounts	To create individual users accounts
To delete 5620 SAM groups	To delete groups
To delete 5620 SAM user accounts	To delete users
To suspend or re-instate 5620 SAM users	To suspend or re-instate users
To change 5620 SAM user passwords as system administrator	To change user passwords as system administrator
To change a 5620 SAM user password as user	To change user passwords as user

8.4 5620 SAM groups and user configuration procedures

This section provides procedures to create and manage groups and users.

Procedure 8-1 To create 5620 SAM user groups

- 1 As admin, choose Security→Manage Security from the 5620 SAM main menu.
The Manage Security form appears.
- 2 Specify:
 - a The creation of a new group by clicking on the Create Group button. The User Group configuration form appears. Go to step 3.
 - b The modification of an existing group:
 - i Click on the Groups tab button.
 - ii Set the filter criteria.
 - iii Click on the Search button.
A list of configured groups appears.
 - iv Choose a group from the list.
 - v Click on the Edit button.
The User Group configuration form appears.
- 3 Click on the General tab button.

- 4 Configure the parameters:
 - i Set the user group name, if applicable.
 - ii Specify a description of the user group using the Description parameter.
 - iii Specify permissions for the group by checking the appropriate group permission check mark boxes. You must specify at least one group permission to allow users who are assigned to that group to have access to a functional area.
- 5 Click on the Apply button to save the changes.
- 6 Validate the action.
- 7 Click on the OK button to close the form.

When you change group permissions, the permissions of all users in the group are altered immediately when you click on the OK button.

Procedure 8-2 To create 5620 SAM user accounts

- 1 As admin, choose Security→Manage Security from the 5620 SAM main menu.
The Manage Security form appears.
- 2 Click on the Users tab button.
- 3 Specify:
 - a The creation of a new user by clicking on the Create User button. The User configuration form appears. Go to step 4.
 - b The modification of an existing user:
 - i Click on the Users tab button.
 - ii Set the filter criteria.
 - iii Click on the Search button.
A list of configured users appears.
 - iv Choose a user from the list.
 - v Click on the Edit button.

The User configuration form appears.

- 4 Configure the parameters.
 - i Specify a user name, if applicable. You cannot use spaces. User names are case sensitive.
 - ii Choose the appropriate group that the user should belong to.
 - Click on the Select button, next to the Security Group parameter. The groupName list form appears.
 - Click on a group from the list.
 - Click on the OK button. The chosen group appears in the Security Group parameter.
 - iii Specify the User State parameter.
 - Choose active to allow the user access.
 - Choose suspended to deny the user access.
 - iv Specify a password of at least 5 characters. You cannot use spaces. Passwords are case sensitive.

The password is the user default password. The user can modify the password by choosing Security→Change Password from the menu bar.
 - v Confirm the password.
 - 5 Click on the OK button to save the changes.
 - 6 Verify the action.
 - 7 Click on the Close button to close the form.
-

Procedure 8-3 To delete 5620 SAM groups

- 1 Choose Security→Manage Security from the menu bar.

The Manage Security form appears.
 - 2 Click on the Groups tab button.
 - 3 Specify a filter to create a filtered list of groups.
 - 4 Choose a group from the Group List.
 - 5 Click on the Remove button.
 - 6 Verify the action.

The group is deleted.
 - 7 Click on the Close button to close the form.
-

Procedure 8-4 To delete 5620 SAM user accounts

- 1 Choose Security→Manage Security from the menu bar.

The Manage Security form appears.

- 2 Click on the Users tab button.
 - 3 Specify a filter to create a filtered list of users.
 - 4 Choose a user from the User List panel.
 - 5 Click on the Remove button.
 - 6 Verify the action.
The user account is deleted.
 - 7 Click on the Close button to close the form.
-

Procedure 8-5 To suspend or re-instate 5620 SAM users

- 1 Choose Security→Manage Security from the menu bar.

The Manage Security form appears.

- 2 Click on the Users tab.
- 3 Specify a filter to create a filtered list of users.
- 4 Choose a user from the user list.
- 5 Click on the Edit button.

The user account configuration form appears.

- 6 Suspend or re-instate the user.
 - a To suspend the user, set the User State parameter to suspended.
 - b To re-instate the user, set the User State parameter to active.
 - 7 Click on the Apply button to save the changes.
 - 8 Verify the action.
-

Procedure 8-6 To change 5620 SAM user passwords as system administrator

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 Security→Manage Security from the menu bar.

The Manage Security form appears.

- 2 Click on the Users tab button.
- 3 Specify a filter to create a filtered list of users.
- 4 Choose a user from the user list.
- 5 Click on the Edit button.

The user account configuration form appears.

- 6 Configure the password parameters.
 - 7 Click on the Apply button to save the changes.
 - 8 Verify the action.
-

Procedure 8-7 To change a 5620 SAM user password as user

Users change their password in the Change Password form.

- 1 Start the 5620 SAM and login using your user name and password.
 - 2 Choose Security→Change Password from the menu bar.
The Password Change form appears.
 - 3 Configure the password parameters.
 - 4 Click on the OK button to save the changes.
 - 5 Click on the Close button to close the form.
-

9 — Security management for 7750 SR users with RADIUS or TACACS+

- 9.1 Security management for 7750 SR using RADIUS AND TACACS+ overview 9-2**
- 9.2 Workflow to manage security for 7750 SR users and RADIUS or TACACS+ 9-3**
- 9.3 7750 SR user and RADIUS or TACACS+ menus 9-4**
- 9.4 7750 SR user and RADIUS or TACACS+ configuration procedures list 9-4**
- 9.5 Device security configuration procedures 9-5**

9.1 Security management for 7750 SR using RADIUS AND TACACS+ 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 to access the managed devices
- configure RADIUS or TACACS+ authentication to control access to the managed devices using 5620 SAM user accounts

RADIUS is an access server AAA protocol. It 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 server. 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 the device.

TACACS+ provides functionality that is similar to RADIUS using a different protocol.

Figure 9-1 shows a Site RADIUS policy form with the General tab button selected.

Figure 9-1 Site RADIUS policy form - General

The screenshot shows a web-based configuration form for a Site RADIUS Policy. The form is titled "Site RADIUS Policy - Default Policy [Edit]" and has four tabs: "General", "Servers", "Local Definitions", and "Faults". The "General" tab is selected. The form contains the following fields and controls:

- Configuration Action:** A dropdown menu set to "Overwrite Existing".
- Displayed Name:** A text field containing "Default Policy".
- Description:** A text field containing "N/A".
- Local:** An unchecked checkbox.
- Administrative State:** A dropdown menu set to "Up".
- Enable Accounting:** A dropdown menu set to "false".
- Enable Authorization:** A dropdown menu set to "false".
- Retry Attempts:** A text input field containing "3".
- Timeout (seconds):** A text input field containing "3".
- Port:** A text input field containing "1812".
- Source Address:** A text input field containing "0.0.0.0".

At the bottom of the form, there are several buttons: "Copy...", "Resync", "Remove" (with a red X icon), "Reset", "OK", "Cancel", and "Apply".

7750 SR users and group permissions

The following general rules apply to 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 filters applied to the managed device apply globally, not per user.
- 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.

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.

9.2 Workflow to manage security for 7750 SR users and RADIUS or TACACS+

- 1 Specify the type of authentication used on the device, for example SHA or MD5.
- 2 Specify the types of access to be granted to each device from the 5620 SAM.
- 3 Create site user profiles based on job classifications and the access needed to the managed devices.
- 4 Create individual site user accounts based on the configured profiles.
- 5 Specify password policies for access to managed devices and for users.
- 6 Manage the user profiles and users:
 - 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.
- 8 Distribute the policies to the managed devices.

9.3 7750 SR user and RADIUS or TACACS+ menus

Table 9-1 lists the device security menu options and their function.

Table 9-1 Device security menu options

Menu option	Function
Security→Site Management Access Filter Manager	Specify the type of access, for example, FTP or Telnet, allowed on the managed devices. These specifications apply to all users that access the device.
Security→Site User Profile Manager	Create profiles of job descriptions and the type of access needed to the managed devices.
Security→Site User Manager	Create user accounts to specify the types of access to the managed devices.
Security→Site Password Policy Manager	Create password policies for users
Security→Site RADIUS Policy Manager	Create policies for RADIUS authentication
Security→Site TACACS+ Policy Manager	Create policies for TACACS+ authentication

9.4 7750 SR user and RADIUS or TACACS+ configuration procedures list

Table 9-2 lists the procedures necessary to create and manage groups and users.

Table 9-2 Device security procedures list

Procedure	Purpose
To create or modify site management access filter policies for managed devices	To specify the level of access allowed on each managed device.
To create user profiles for managed device access	To specify profiles, based on job classifications, for the types of users who need access to the managed devices.
To create, modify, and manage user accounts for access to managed devices	To create users, based on the created profiles, that the managed device can use to authenticate Telnet, SNMPv3, FTP, and console access.
To specify or modify password policies	To specify the password policies to create, manage, and modify user passwords.
To create RADIUS access policies	To create RADIUS policies
To create TACACS+ access policies	To create TACACS+ policies
To distribute policies	To distribute created policies to one or more managed devices.

9.5 Device security configuration procedures

This section provides procedures to create and manage security on the managed devices.

Procedure 9-1 To create or modify site management access filter policies for managed devices

Site management access filters:

- restrict the type of management access allowed
- specify strict underlying connection protocol usage, and the accepted IP addresses and ports that can access the device

- 1 As admin, choose Security→Site Management Access Filter Manager from the 5620 SAM main menu.

The Site Management Access Filter Manager form appears.

- 2 Specify:
 - a A filter to search for and edit an 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 Edit button.
 - b Create a new filter by clicking on the Create Management Access filter button.

When you create a new filter, the Site Management Access Filter (Create) form appears.

- 3 From the General tab, enter a name and description for the site management access filter using the Displayed Name and Description parameters.
- 4 Specify the Default Filter Action parameter to determine which action is performed when there are no matching management access filters. The default action is applied to any packets that do not satisfy any of the match criteria in the management access filters. The options are:
 - none to specify that no filtering is done
 - permit to specify that packets that do not match the selection criteria of the filter entries are permitted
 - deny to specify that packets that do not match the selection criteria are denied
 - Deny Host Unreachable to specify that packets that do not match the selection criteria are denied and a host unreachable message is sent
- 5 Click on the Entries tab button.
- 6 Click on:
 - a The Add button to add a new site entry.
 - b An entry in the list and click on the Edit button to modify an existing entry.

The Site MAF Match Entry (Create) form appears when you create a new entry.

- 7 Specify an ID for the site MAF match entry, or have an ID auto-assigned.
- 8 Specify a name and description using the Displayed Name and Description parameters.
- 9 Set the properties of the site MAF match entry, as shown in Figure 9-2

Figure 9-2 Site management access filter form

- i Specify the filter action using the Action parameter.
 - none to specify that no filtering is done
 - permit to specify that packets that match the configured selection criteria of the filter entries are permitted
 - deny to specify that packets that match the configured selection criteria are denied and an ICMP host unreachable message is sent
 - Deny Host Unreachable to specify that packets that match the configured selection criteria are denied and a host unreachable message is sent
- ii Specify the source IP address and source IP Mask of the request.
- iii Specify the Source Port Type parameter to indicate that incoming packets are restricted and must be sent by the following port type to satisfy the match criteria.
 - any
 - cpm
 - port
 - lag
- iv Specify the Source Port ID parameter, in the format slot/daughtercard/port, to set the source port. For example, to configure port 3 on daughter card 2 on card 6, enter 6/2/3. LAGs are specified by the LAG ID.
- v Specify the Destination Port and Destination Port Mask parameters to indicate the destination UDP or TCP port number.
- vi Specify the Protocol parameter to indicate which protocol is to be used as a match filter.

- vii Click on the Apply button to save the changes.

The new site MAF match entry appears in the list form.

- 10 Click on the Apply button to save the changes.
 - 11 Verify the action.
 - 12 Repeat for each site management access filter you want to create or modify.
 - 13 Click on the Apply button to save the changes.
-

Procedure 9-2 To create user profiles for managed device access

Site user profiles are used to specify which commands or command groups are permitted or denied on the managed device from the 5620 SAM.

- 1 As admin, choose Security→Site User Profile Manager from the 5620 SAM main menu.

The Site User Profile Manager form appears.
- 2 Specify:
 - a A filter to search for and edit and existing site user profiles. Choose a site user profile from the list and click on the Edit button.
 - b A new site user profile by clicking on the Create Site User Profile button.

The Site User Profile (Create) form appears.
- 3 From the General tab, enter a name and description for the site user profile using the Displayed Name and Description parameters.
- 4 Specify the Default Profile Action parameter for the profile.
 - deny
 - allow
 - none
- 5 Click on the Entries tab button.
- 6 Click on:
 - a The Add button to add a new site entry.
 - b An entry in the table and click on the Edit button to modify an existing entry.

The Site User Profile Match Entry (Create) form appears when you create a new entry.
- 7 Specify a name and description for the user profile match entry using the Displayed Name and Description parameters.

- 8 Specify an action using the Action parameter.
 - deny to deny use of the match string
 - allow to allow the use of the match string
 - none to not specify an action
- 9 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”.
- 10 Click on the Apply button to save the changes. The site user profile match entry appears in the list form.
- 11 Verify the action.
- 12 Click on the OK button to close the form.
- 13 Repeat for each required site user profile.

Procedure 9-3 To create, modify, and manage user accounts for access to managed devices

Create user accounts:

- to create an user account on the device
- as a backup for managed device access when the authentication servers are offline or cannot be used
- to specify the types of access allowed on the managed devices, for example, Telnet, SNMPv3, FTP, or console



Note — System Administrators can click on the Statistics tab to view information about the configured user’s actions.

- The number of login attempts and the number of successful login attempts.
- The last time that the password was changed.

You can also view the login statistics for all users by listing all existing users in the filter form and scrolling across the list of users to the login and password information columns.

- 1 As admin, choose Security→Site User Manager from the 5620 SAM main menu.
The Site User Manager form appears.
- 2 Specify:
 - a A filter to search for and edit an existing site user account.
 - b A new site user account by clicking on the Create Site User button.

When you create a new site user account, the Site User (Create) form appears with the General tab button selected.

- 3 Specify a name and description for the user account using the User Name and Description parameters.
- 4 Specify the permissions for the user.
 - i Select one or more check boxes to enable access to:
 - SNMP
 - FTP
 - console (serial port or Telnet access)

Figure 9-3 shows the form with all permissions enabled.

Figure 9-3 Site user create form - General

The screenshot shows a web-based configuration form titled "Site User, [Create]". The "General" tab is selected. The form contains the following elements:

- Configuration Action:** A dropdown menu set to "Merge With Existing".
- User Name:** A text input field.
- Description:** A text input field.
- Set New Password (Console and/or FTP):** Two text input fields for "Password:" and "Confirm Password:".
- Permissions:** A section with three checked checkboxes: "snmp", "ftp", and "console".
- Home Directory:** A text input field containing "name of directory".
- Restrict to Home:** A dropdown menu set to "true".
- Console Login Exec File:** A text input field.
- Console Cannot Change Password:** A dropdown menu set to "true".
- Console New Password At Login:** A dropdown menu set to "false".

At the bottom of the form are four buttons: "Reset", "OK", "Cancel", and "Apply".

- ii Enter a home directory on the managed device where the user first goes when accessing the device.
 - iii Specify whether the user can access other directories from the home directory.
 - iv Specify whether the user can change the password when logging in to the console.
- 5 Specify a new password for the user's access to the managed device when FTP or console access is used.

- 6 When a user has console permission, you can configure the parameters in the Console Profile tab.
 - i Click on the Console Profile 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 next to a profile number. The Select Site User Profile form appears.

Default profiles and the profiles created in Procedure 9-2 are listed.
 - iii Choose a profile from the list.
 - iv Click on the OK button.

The profile name appears next to the profile number.
- 7 When a user has SNMPv3 permissions, you can configure the authentication parameters.
 - i Click on the SNMP v3 tab button.
 - ii Specify the authentication protocols. Authentication checks are used by the managed device to ensure that the SNMP messages sent from the 5620 SAM have not been tampered with.



Note — The authentication protocol should match the authentication used on the devices where the accounts reside.

- No Authentication specifies that no checks, except a permission check of the user account, is performed.
 - MD5 specifies that the authentication protocol can be HMAC-MD5-96 or HMAC-SHA-96. The password length is specified in the Set New Authentication Password parameters.
 - SHA specifies that the authentication protocol can be either HMAC-MD5-96 or HMAC-SHA-96. The password length is specified in the Set New Authentication Password parameters.
- iii Specify the privacy protocol. This parameter specifies the type of SNMP packet encryption used.
 - No Privacy specifies not to perform SNMP packet encryption.
 - DES specifies the DES key for SNMP encryption. The password length is specified in the Set New Privacy Password parameters.
 - iv Click on the OK button to save the changes.
 - v Verify the action.
- 8 Click on the Apply button to save the changes.
-

Procedure 9-4 To specify or modify password policies

Create password policies:

- to define rules that passwords must conform to on the devices where access policies are in effect
- specify the details of the passwords

- 1 As admin, choose Security→Site Password Policy Manager from the 5620 SAM main menu.

The Site Password Policy Manager form appears.

- 2 Specify:

- a A filter to search for and edit an existing password policy.
- b A new password policy by clicking on the Create Site Password Policy button.

When you create a new password policy, the Site Password Policy (Create) form appears with the General tab button selected, as shown in Figure 9-4.

Figure 9-4 Site password create form - General

The screenshot shows the 'Site Password Policy, [Create]' window with the 'General' tab selected. The 'Configuration Action' is set to 'Merge With Existing'. The 'ID' field contains '0' and 'Auto-Assign ID' is checked. The 'Name' and 'Description' fields are empty. In the 'Properties' section, 'Special Characters' and 'Mixed Case' are checked, while 'Numeric Characters' is unchecked. 'Lockout Time (minutes)' is set to 10. 'Password Never Expires' is unchecked. 'Days Before Expiration' is 500, 'Minimum Length' is 6, 'Maximum Attempts' is 3, and 'Maximum Attempts Time (minutes)' is 5. The 'Authentication Order' section shows three dropdown menus: 'radius', 'tacplus', and 'local'. At the bottom, there are 'Reset', 'OK', 'Cancel', and 'Apply' buttons.

- 3 Specify a name and description for the password policy using the Name and Description parameters.

- 4 Specify the password policies.
 - i Specify the types of allowed characters in the password using the appropriate check boxes.
 - Special Characters to specify that at least one special character must be included in the password, for example &
 - Numeric Characters to specify that at least one number must be included in the password
 - Mixed Case characters to specify that at least one uppercase and one lowercase character must be included in the password
 - ii Specify the Minimum Length parameter for the password to determine minimum password length.
 - iii Specify whether the password expires using the Password Never Expires check box. If the password can expire, specify the Days Before 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.
 - iv Use the Maximum Attempts parameter to specify the maximum number of attempts that the user can try to enter with the password, and the Maximum Attempts Time (minutes) parameter to specify the number of attempts allowed within a specified time.
 - v 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.
 - 5 Specify the types and order of password authentication that will be used to verify the user account password using the three Authentication Order parameters.

Set the order from the most preferred method of authentication to the least preferred method of authentication.

 - none to specify not authentication
 - radius to specify RADIUS server password authentication
 - tacplus to specify TACACS+ server password authentication
 - local to specify locally-managed device password database authentication
 - 6 Click on the OK button to save the changes.
-

Procedure 9-5 To create RADIUS access policies

See to the appropriate RADIUS documentation for more information about configuring RADIUS servers.

- 1 Choose Security→Site RADIUS Policy Manager from the 5620 SAM main menu.

The Site RADIUS Policy Manager form appears.
- 2 Specify:

- a A filter to search for and edit an existing RADIUS access policy.
- b A new RADIUS access policy by clicking on the Create Site RADIUS Policy button.

When you create a new RADIUS access policy, the Site RADIUS Policy (Create) form appears with the General tab selected, as shown in Figure 9-1.

- 3 Specify a name and description for the RADIUS access policy using the Displayed Name and Description parameters.
 - 4 Set the Administrative State to Up to use the configured RADIUS server for authentication.
 - 5 Set the Enable Accounting to true to enable RADIUS accounting.
 - 6 Set the Enable Authorization to true to enable RADIUS authorization parameters.
 - 7 Specify the number of retry attempts where the RADIUS server is contacted to perform authorization using the Retry Attempts parameter.
 - 8 Specify the timeout range to determine how many seconds the managed device waits for a response from the RADIUS server using the Timeout (seconds) parameter.
 - 9 Specify the TCP port of the RADIUS server that will be contacted using the Port parameter.
 - 10 Specify the IP address of the RADIUS server using the Source Address parameter.
 - 11 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 Add button.

The Site RADIUS Server (Create) form appears.
 - ii Specify an ID for the RADIUS server.
 - iii Specify a name and description for the RADIUS server using the Displayed Name and Description parameters.
 - iv Specify the IP address of the RADIUS server using the Address parameter. Each RADIUS server must have its own different IP address.
 - v Specify the Secret parameter. The Secret parameter value must match the secret password value on the RADIUS server.
 - vi Click on the OK button to save the changes.
 - 12 Click on the Apply button to save the changes.
-

Procedure 9-6 To create TACACS+ access policies

- 1 Choose Security→Site TACACS+ Policy Manager from the 5620 SAM main menu.

The Site TACACS+ Policy Manager form appears.

- 2** Specify:
 - a** A filter to search for and edit an existing TACACS+ access policy.
 - b** A new TACACS+ access policy by clicking on the Create Site TACACS+ Policy button.

When you create a new TACACS+ access policy, the Site TACACS+ Policy (Create) form appears.

- 3** Specify a name and description for the TACACS+ access policy using the Displayed Name and Description parameters.
- 4** Set the Administrative State parameter to Up to use the configured TACACS+ server for authentication.
- 5** Set the Enable Accounting parameter to true to enable TACACS+ accounting.
- 6** Specify the Accounting Type parameter to determine the type of accounting when accounting is enabled.
 - start and stop
 - stop only
- 7** Set the Enable Authorization parameter to true to enable TACACS+ authorization parameters.
- 8** Specify the Timeout (seconds) parameter range to determine how many seconds the managed device waits for a response from the TACACS+ server.
- 9** Select the Single Connection check box to specify a single connection. This allows a single connection to the TACACS+ server to stay up, rather than set up a new connection for each authentication event.
- 10** Specify the IP address of the TACACS+ server using the Source Address parameter.
- 11** 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 Add button.

The Site TACACS+ Server (Create) form appears.

- ii** Specify an ID for the TACACS+ server.
- iii** Specify a name and description for the TACACS+ server using the Displayed Name and Description parameters.
- iv** Specify the IP address of the TACACS+ server using the Address parameter. Each TACACS+ server must have its own different IP address.
- v** Specify the Secret parameter. The secret value must match the secret value on the TACACS+ server.
- vi** Click on the OK button to save the changes.

- 12 Click on the Apply button to save the changes.
-

Procedure 9-7 To distribute policies

- 1 Create policies, as described in Procedures 9-1 to 9-6.
 - 2 Choose the appropriate policy from the Security→*option* menu.
The appropriate policy filter form appears.
 - 3 Set the filter criteria, if applicable.
 - 4 Click on the Search button.
A policy list appears.
 - 5 Choose a policy from the list.
 - 6 Click on the Distribute button.
The Distribute form appears.
 - 7 Specify which devices to distribute the policy to.
 - i Click on one or more devices in the left hand available nodes column.
 - ii Click on the right-facing arrow.
The selected device(s) move to the right-hand column.
 - 8 Click on the Distribute button.
The policy is distributed to the selected device(s).
-

10 — Deployment and site backup/upgrade management

- 10.1 Deployment and site backup/upgrade overview 10-2**
- 10.2 Workflow for deployment and site backup/upgrade 10-2**
- 10.3 Deployment and site backup/upgrade menu 10-2**
- 10.4 Deployment and site backup/upgrade procedures list 10-3**
- 10.5 Deployment and site backup/upgrade procedures 10-3**

10.1 Deployment and site backup/upgrade overview

The 5620 SAM deployment and site backup/upgrade form is used by system administrators to:

- configure a 5620 SAM-to-node deployment policy
- troubleshoot the status of a configuration deployment
- schedule a backup or restore for a node database
- upgrade the node software image
- view the status of a backup, restore, or upgrade

When you save a configuration using the 5620 SAM, the configurations are stored and sent to the node according to the 5620 SAM-to-node deployment policy. The deployment policy parameters include the:

- frequency of the deployment
- number of retries by the 5620 SAM to make the deployment

You can specify whether to save a currently running configuration file to a compact Flash device, or an FTP remote location. See the “Boot Options” chapter in the *7750 SR OS System Guide* for more information. The “Service Management” section in the *7750 SR OS System Guide* describes how to modify and save a configuration.

10.2 Workflow for deployment and site backup/upgrade

- 1 Use the 5620 SAM to configure a deployment policy. The deployment policy specifies the frequency that the 5620 SAM sends configurations to the node.
- 2 Troubleshoot a configuration deployment, as required.
- 3 Use the CLI to specify whether to save a currently running configuration file to a compact Flash device or an FTP remote location.
- 4 Use the CLI to configure the Boot Option File (BOF) persist parameter.
- 5 Configure the backup and restore parameters for the node.
- 6 Upgrade the node software image.
- 7 View the status of the backup, restore, or upgrade.

10.3 Deployment and site backup/upgrade menu

Table 10-1 lists the mediation menu that you use to open the Deployment and Site Backup/Upgrade form.

Table 10-1 5620 SAM mediation menu

Menu option	Function
Mediation→Deployment and Site Backup/Upgrade	Open the mediation policy form and configure a mediation policy

10.4 Deployment and site backup/upgrade procedures list

Table 10-2 lists the procedures that you can perform from the Deployment and Site Backup/upgrade form.

Table 10-2 Database management procedures list

Procedure	Purpose
To configure a 5620 SAM-to-node deployment policy	Configure a deployment policy.
To troubleshoot a configuration deployment	Troubleshoot a configuration deployment.
To schedule a device backup	Configure backup and restore parameters.
To start an immediate backup or restore	Start an immediate backup or restore.
To upgrade the node software image	Upgrade the node software image.
To view the status of the backup, restore, or upgrade	View the status of the backup, restore or upgrade.

10.5 Deployment and site backup/upgrade procedures

Use the following procedures to perform deployment and site backup/upgrade tasks.

Procedure 10-1 To configure a 5620 SAM-to-node deployment policy

- 1 Choose Mediation→Deployment and Site Backup/Upgrade from the 5620 SAM main menu.
The Deployment and Site Backup/Upgrade form appears.
- 2 Click on the Deployment Policy tab button. Figure 10-1 displays the Deployment and Site Backup/Upgrade form with the Deployment Policy tab button selected.

Figure 10-1 Deployment and Site Backup/Upgrade form - Deployment Policy

3 Configure the parameters.



Note — Alcatel recommends that you set the Deployment Mode parameter to the Deployed through SNMP option. When you set the Deployment Mode parameter to the No Deployment option, 5620 SAM configurations remain on the 5620 SAM, and are not sent to the device.

- i A configuration file of the changes made to the routers using the 5620 SAM can be generated every time the changes are made to the device. You can perform an autosave using the Auto Save parameters, or a scheduled save using the Schedule Save parameters.
 - ii You can determine a policy for how often the 5620 SAM tries to redeploy to the device. Specify the Retry Scheme, Retry Frequency, and Retry Threshold parameters.
- 4 Click on the OK button to save the deployment policy.
- 5 Verify the action.
- 6 Close the form.

Procedure 10-2 To troubleshoot a configuration deployment

The Deployers tab displays configuration deployments that failed, and allows you to view information about the deployment. From the Deployers tab, you can clear the configuration, override the error to force the configuration to be downloaded to the node, or suspend or resume retries to the node.

- 1 Choose Mediation→Deployment and Site Backup/Upgrade from the 5620 SAM main menu.

The Deployment and Site Backup/Upgrade form appears.

- 2 Click on the Deployers tab.
- 3 Choose a deployer from the list.
- 4 Double-click the deployer for more information about the configuration deployment.

The deployer form appears, indicating the deployer ID.

- 5 Review the deployer information, including the state value, which gives information about deployer fault conditions. Information about the configuration being attempted by the deployer is shown in the objects list.

- i Click on a row in the objects list.

- ii Click on the Edit button.

The object change form for the configuration change being attempted by the deployer appears.

- iii Review the additional information in the attributes list.

See the *Alcatel 5620 SAM Network Management Troubleshooting Guide* and *Alcatel 5620 SAM-O OSS Interface Developer Guide* for more information about troubleshooting deployer issues.

Procedure 10-3 To schedule a device backup

When the 5620 SAM does a backup of node configurations, the 5620 SAM FTPs to the node and gets the:

- node bof file (bof.cfg)
- primary-config specified in the bof
- index file (primary-config with a .ndx extension)

Before you schedule a backup, you must:

- have admin user access on the 5620 SAM
- have a user account with FTP access on the managed device
- use the CLI to enable the BOF persist parameter by typing the command: <bof persist on> and saving the configuration. See the “Boot Options” chapter in the *7750 SR OS System Guide* for more information.

- 1 Choose Mediation→Deployment and Site Backup/Upgrade from the 5620 SAM main menu.

The Deployment and Site Backup/Upgrade form appears.

- 2 Click on the Backup/Restore Policy tab. Figure 10-2 displays the Deployment and Site Backup/Upgrade form with the Backup/Restore Policy tab button selected.

Figure 10-2 Deployment and Site Backup/Upgrade form - Backup/Restore Policy

The screenshot shows a web-based configuration interface for the 5620 SAM. The title bar reads "Deployment and Site Backup/Upgrade". There are six tabs: "Deployers", "Deployment Policy", "Backup/Restore Policy" (which is selected), "Backup/Restore Status", "Software Upgrade Policy", and "Software Images".

The "Backup/Restore Policy" tab contains the following configuration options:

- Backup Mode:** A dropdown menu set to "Uploaded by 5620 SAM Server through FTP".
- FTP User Name:** A text input field containing "admin".
- FTP User Password:** A text input field containing "*****".
- Auto Reboot After Successful Restore:** A checked checkbox.
- Backup Triggering:** A sub-section containing:
 - Scheduled Backup Scheme:** A dropdown menu set to "Every Scheduled Interval".
 - Scheduled Backup Frequency:** A dropdown menu set to "24 hours".
 - Scheduled Backup Threshold (operations):** A text input field containing "0".
 - Auto Backup Scheme:** A dropdown menu set to "No Auto-backup".
 - Auto Backup Threshold (operations):** A text input field containing "0".
- Backup Settings:** A sub-section containing:
 - CLI Config File Mode:** A dropdown menu set to "Always".
 - Boot Option File Mode:** A dropdown menu set to "Always".
 - Boot Option File Path:** A text input field containing "/cf3:/bof.cfg".
 - 5620 SAM Server Repository Root Path:** A text input field containing "/sr-backup/".

At the bottom right of the form are four buttons: "Reset", "OK", "Cancel", and "Apply".

- 3 Configure the parameters.
 - i Specify the Backup Mode parameter. Since the 5620 SAM opens an FTP session with the device, the FTP User Name and FTP User Password must match a user account on the device where FTP access is enabled for that user. Enter your FTP user name and password. To enable FTP access for a device user account:
 - access the node using CLI
 - type: configure system security user *user name*, where *user name* is the user account being given FTP access, and enter a password, if required
 - type: access ftp
 - ii Specify whether to perform a reboot after the database is restored to the device by clicking on the Auto Reboot After Successful Restore check box.
 - iii You can perform scheduled backups based on a time interval or perform automatic backups based on the number of router configurations performed from the 5620 SAM server.

Specify the backup scheme, frequency, and interval using the appropriate parameters.

iv Specify the backup settings.

Configure the Boot Option File (BOF) Path parameter to specify the location of the BOF. A BOF specifies where the system searches for runtime images, configuration files, and other operational parameters during system initialization. BOF parameters can be modified. Changes can be saved to a specified compact flash. The BOF must be located in the root directory of either an internal or external compact flash local to the system and have the mandatory filename of `bof.cfg`.

Specify both the BOF settings and the repository on the 5620 SAM where the backed-up database is stored. The default directory is on the 5620 SAM server, in the `..bin\sr-backup\router-id` directory, where *router-id* is the router ID and system address for the router.

4 Click on the OK button to save the backup and restore configuration.

Procedure 10-4 To start an immediate backup or restore

When you start an immediate backup, you back up the device database based on the backup configuration that you specified in Procedure 10-3.

When you restore a database, it is restored based on the last configuration file that you backed up.

1 Choose Mediation→Deployment and Site Backup/Upgrade from the 5620 SAM menu.

The Deployment and Site Backup/Upgrade form appears.

2 Click on the Backup/Restore Status tab.

All managed devices are listed.

3 Choose a device from the list.

4 Click on the View button.

Information about the backed-up or restored router databases are displayed.

5 Close the form.

6 Return to the Deployment and Site Backup/Upgrade form.

7 Click on the Backup button or Restore button, depending on the function that you want to perform.

Procedure 10-5 To upgrade the node software image

The node software image you use for the upgrade depends on the type of device. For example:

- 7750 SR-1 nodes require the both.tim file, which must be stored in a separate directory below the root (by default, the sr-images) directory
- 7750 SR-4 and 7750 SR-12 nodes require the cpm.tim file and the iom.tim file, which can be stored in the same directory below the root (by default, the sr-images) directory

- 1 Choose Mediation→Deployment and Site Backup/Upgrade from the 5620 SAM main menu.

The Deployment and Site Backup/Upgrade form appears.

- 2 Click on the Software Upgrade Policy tab.
- 3 Configure the Repository Root on 5620 SAM Server parameter by typing the full path of the directory on the 5620 SAM that contains the image. For example:

```
c:\sr-images\TiMOS_2.0.1_R4_for_SR7
```

In this example, the directory name identifies the storage location for node software image files for a Release 2_0_4 version of the seven-slot 7750 SR.

- 4 Click on the Apply button.
- 5 Configure the CFlash Image Root Path and the CFlash Backup Root Path, where the image is to be downloaded to the device and where the image is backed up, using the following formats:

```
cf3: /<directory name>
```



Note — When you perform a device software upgrade, ensure that the correct device software image directory is selected, for example, TiMOS_2.0.1_R4_for_SR7 for a Release 2_0_4 version of the seven-slot 7750 SR.

- 6 Specify whether to reboot the device after the updated image is downloaded using the Auto-Reboot After Successful Upgrade check box.
- 7 Click on the Software Images tab.
- 8 Click on the Refresh button.
- 9 Click on the OK button.
- 10 Click on the View button to check the location of the CPM and IOM software image files directory names. For example, the TiMOS_2.0.1_R4_for_SR7 would be listed under the CPM and IOM card software version tabs, and the applicable *.tim files would be listed under the CPM and IOM Image File Path tabs.
- 11 Click on the Upgrade Sites button.

A list of sites appears.

- 12 Choose a site from the list.
- 13 Click on the OK button.

The upgrade starts. See Procedure 10-6 for information about viewing the status of an upgrade.



Note — The amount of time to perform the upgrade depends on the shelf size of the device. The CPM Sync and Reboot status indicates that the update is occurring and may take many minutes to complete, and does not indicate a problem.

Procedure 10-6 To view the status of the backup, restore, or upgrade

- 1 Choose Mediation→Deployment and Site Backup/Upgrade from the 5620 SAM menu.

The Deployment and Site Backup/Upgrade form appears.

- 2 Click on the Backup/Restore Status tab.

A list of the backups and restores appears. The Restore State column of the backup or restore may be: Transferring Files, Pending, Reboot, CMP Sync and Reboot, Success, Not Attempted, Save Config, or Failure. The timestamp of an upgrade is also displayed.

- 3 Double-click on a row to view the backup and restore configuration information.

Click on the appropriate tab for more information about:

- backup and restore status
 - the software images stored in backup folders
 - configuration or upgrade states
 - alarms raised because of backups, restores, or mediation configurations
-

11 — 5620 SAM database manager

- 11.1 5620 SAM database manager overview 11-2**
- 11.2 Workflow to manage the 5620 SAM database 11-2**
- 11.3 5620 SAM database menu 11-2**
- 11.4 5620 SAM database procedures list 11-2**
- 11.5 5620 SAM database procedures 11-3**

11.1 5620 SAM database manager overview

The 5620 SAM database manager is used by system administrators to perform traditional database management system tasks on the workstation being used as the 5620 SAM database. You need to have the clearance to update the database, as either an admin or Oracle dba user, to:

- view the Oracle database data and statistics used by the 5620 SAM
- perform database analysis
- backup a 5620 SAM database
- view the results of a 5620 SAM database analysis or backup

11.2 Workflow to manage the 5620 SAM database

- 1 Autodiscover the network. The database of the managed devices is stored in the 5620 SAM database.
- 2 Perform regular database management according to company policy:
 - i Monitor the database as required.
 - ii Analyze the database as required. Alcatel recommends that as the database grows, tablespaces should be analyzed with increasing frequency.
 - iii Back up the database as required. Alcatel recommends that you back up the database at least once a day.

11.3 5620 SAM database menu

Table 11-1 lists the database menu and its function.

Table 11-1 5620 SAM database menu

Menu option	Function
Policies→Database Manager	Set database policies using the Database Manager form.

11.4 5620 SAM database procedures list

Table 11-2 lists the procedures to execute database management tasks.

Table 11-2 Database management procedures list

Procedure	Purpose
To view general database statistics	View general details about the database.
To analyze the database	Perform a database analysis to troubleshoot a database problem.
To back up the database	Perform a scheduled backup of the database and store the latest version of the database for analysis or for future use

11.5 5620 SAM database procedures

Use the following procedures to perform database management tasks.

Procedure 11-1 To view general database statistics

Database statistics provide general information about the Oracle database that stores 5620 SAM data.

- 1 Choose Policies→Database Manager from the 5620 SAM main menu.

The Database Manager form appears. Figure 11-1 shows the Database Manager form with the General tab selected.

Figure 11-1 Database Manager form - General

The screenshot shows a window titled "Database Manager - database-manager [Edit]". It has three tabs: "General", "Analysis", and "Backup". The "General" tab is selected. The main area is titled "Primary Database" and contains several fields with their values:

- Database Name: srm2dot0
- DBID: 3276232674
- Creation Time: 2004-03-06 18:13:54.0
- Version: Oracle9i Release 9.2.0.4.0 - Production
- DB Server: 138.120.135.105
- Open Mode: READ WRITE
- Archive Log Mode: ARCHIVELOG

At the bottom right, there are three buttons: "Analyze...", "Backup...", and "Cancel".

- 2 View the following information from the General tab button:
 - Database Name created using the installer
 - DBID, which is the database ID of the Oracle database
 - Creation Time of the database using the installer
 - Version of the installed Oracle database
 - DB Server IP address of the networkstation containing the database server
 - Open Mode, which specifies the type of access available to the database, either read or read and write
 - Archive Log Mode, either to archive the log or not to archive the log as specified during installation
-

Procedure 11-2 To analyze the database

You can analyze the database to check the integrity of the database. Clean tablespaces in the database are essential for quick and efficient queries to the database. Analyze the tables more frequently as more data is added to the database.

- 1 Choose Policies→Database Manager from the 5620 SAM menu.

The Database Manager form appears.
- 2 Click on the Analysis tab button.
 - a Click on the Schedule analysis button to schedule an analysis and define the analysis parameters.

The Define Analysis parameters form appears.

 - i The Analysis Frequency parameter specifies the interval. For example, setting the Analysis Frequency parameter to 5 and setting the Frequency Unit parameter to hour means an analysis is performed every 5 hours.
 - ii The Frequency Unit parameter specifies the unit of time. The options are never, minute, hour, or week.
 - iii Click on the Next button.

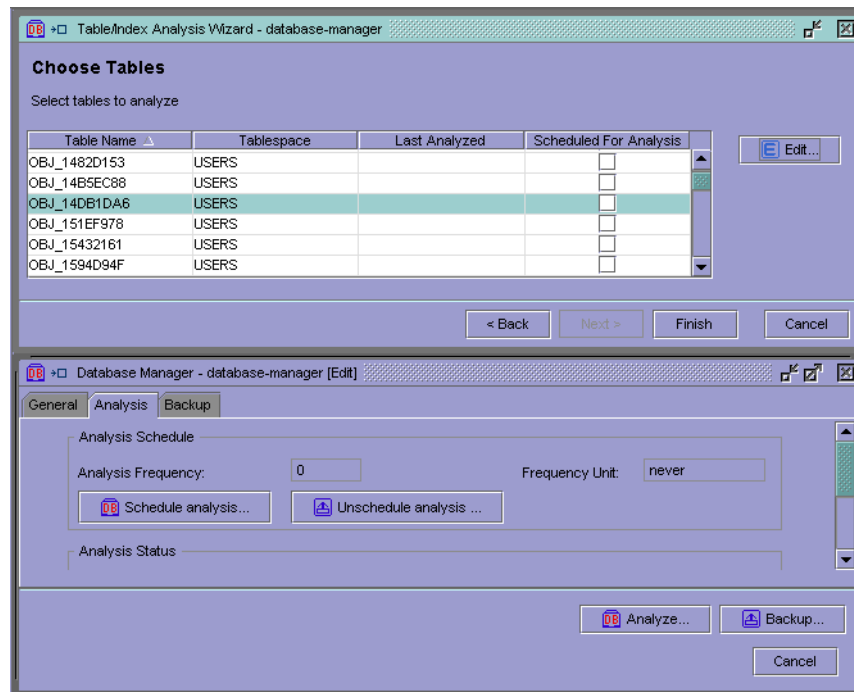
The Choose Tables form appears.
 - iv Specify the database tables that need analysis.



Note — Contact your Alcatel support representative for more information about the types of data stored in each database table type.

Shift-click to select multiple adjacent rows. CTRL-click rows to select multiple non-adjacent rows. Figure 11-2 shows the tables.

Figure 11-2 Database table list form



- v Click on the Finish button.

An operation status message appears.

- b Click on the Analysis button to perform an analysis without a schedule.
- i Choose the tables to be analyzed, if applicable.



Note — Contact your Alcatel support representative for more information about the types of data stored in each database table type.

- ii Click on the Finish button.

An operation status message appears.

- iii Click on the Close button.

- 3 Analysis status information is shown on the Analysis tab of the Database Manager form.

Table analysis provides information such as:

- whether an analysis schedule has been configured
- whether the last analysis succeeded or failed
- the next scheduled analysis time
- when the last successful analysis was completed

Details about the analysis, such as the number of tablespaces analyzed and the state of those tablespaces, are stored in Oracle catalog tables. See the Oracle documentation for information about querying the Oracle database to view the results, and to perform other database management tasks.

Procedure 11-3 To back up the database

Back up the 5620 SAM database as a preventive measure in case there is a problem with network management system or the database. A database backup provides a snapshot of the database. You can use the backup to restore network data:

- if you want to move a database from one workstation to another
- to recover from hardware or software errors
- to provide a clean copy of the database before performing a new installation or upgrade
- as a preventative measure before making major changes to the network, or deploying a large number of new network devices

You can restore a database using the database installer, as described in the *Alcatel 5620 SAM Installation Guide*.



Note 1 — The database must be in ARCHIVELOG mode to perform a backup.

Note 2 — During a database backup, the performance of database-related operations from the GUI or the XML OSS interface may be affected. Alcatel recommends performing database backups during low-activity windows.

- 1 Choose Policies→Database Manager from the 5620 SAM main menu.
The Database Manager form appears.
- 2 Click on the Backup tab button.
- 3 Specify how to perform backups, either using a scheduled or an unscheduled method.
 - a Click on the Schedule backup button to schedule an backup.
The Define Backup Schedule form appears.
 - i Define the backup schedule. The Backup Frequency parameter specifies at what interval the backup is done. For example, setting the Backup Frequency parameter to 5 and setting the Frequency Unit parameter to hour means a backup is performed every 5 hours.
 - ii The Frequency Unit parameter specifies the unit of time. The options are never, minute, hour, or week.
 - iii Click on the Next button.

- iv Specify the database backup root backup directory destination using the Backup Directory parameter. Type the path of the backup directory. For scheduled backups, the backup databases are stored in up to three subdirectories, to ensure multiple versions of the database are available.



Note — Ensure that the backup location is not tampered with, overwritten, and has enough space to contain the database. For regularly scheduled backups, ensure that there is enough space for numerous backup copies of the database.

- v Click on the Finish button.

An operation status message appears.

- b Click on the Backup button to perform a backup without a schedule.

The Define Backup Directory form appears.

- i Specify the database backup root backup directory destination using the Backup Directory parameter. Type the path of the backup directory. For scheduled backups, the backup databases are stored in up to three subdirectories, to ensure multiple versions of the database are available.



Note — Ensure that the backup location is not tampered with, overwritten, and has enough space to contain the database. For regularly scheduled backups, ensure that there is enough space for numerous backup copies of the database.

- ii Click on the Finish button.

An operation status message appears.

- 4 Backup status information is shown on the backup tab of the Database Manager form.

Backup status provides information such as:

- whether a backup schedule has been configured
- whether the last backup succeeded or failed
- the next scheduled backup time
- when the last successful and attempted backup was completed
- directory of the last successful backup

- 5 Click on the Close button.



Note — After backing up and restoring a database, you must perform a full resync of the network to discover any changes to the managed devices, or any new managed devices.

12 — Using CLI from the 5620 SAM

- 12.1 CLI overview 12-2**
- 12.2 Workflow to use the CLI 12-2**
- 12.3 CLI menus 12-2**
- 12.4 CLI procedure list 12-3**
- 12.5 CLI procedures 12-3**

12.1 CLI overview

Most device management functions can be performed using the 5620 SAM client GUI. Experienced operators and system administrators can launch CLI sessions to managed devices, such as the 7750 SR, from the same workstation or PC that runs the 5620 SAM client GUI. The CLI can be used to:

- validate actions performed on the GUI
- perform configurations not available from the GUI
- troubleshoot using managed device log files
- script a complex sequence of CLI commands and then run the script using a command button

Access to CLI commands is controlled by user account permission privileges. Permissions are set when security is configured on the managed device or by using 5620 SAM security configuration forms. See chapter 9 for more information about setting device access privileges.

See the *7750 SR OS System Guide* chapter “CLI Usage” for more information about the 7750 SR CLI structure and usage. See the appropriate device hardware documentation for applicable CLI commands. The following CLI commands are below root in the CLI hierarchy for the 7750 SR:

- admin
- bof
- configure
- environment
- file
- monitor
- help
- password
- show
- clear
- debug
- tools

12.2 Workflow to use the CLI

- 1 Ensure that the user logged in to the 5620 SAM client GUI has console access account privileges to the managed devices.
- 2 Launch a CLI session and configure CLI preference settings.
- 3 Launch a CLI session and log in to the managed device.
- 4 Configure CLI scripts.
- 5 Run CLI scripts according to user privilege and job function.

12.3 CLI menus

Table 12-1 lists the 5620 SAM CLI menus.

Table 12-1 5620 SAM CLI menus

Menu option	Function
Options→SR CLI→Telnet Session	To launch a Telnet console session
Options→SR CLI→SSH Session	To launch an SSH console session
From the navigation tree, Equipment→ <i>Device</i> right-click contextual menu CLI→ <i>option</i> , where <i>option</i> is Telnet or SSH	To immediately connect using the IP address of the device, and display the CLI login window

12.4 CLI procedure list

Table 12-2 lists the procedures to use, configure, and manage CLI.

Table 12-2 5620 SAM CLI procedures list

Procedure	Purpose
To launch a CLI session	To open a Telnet or SSH console, and communicate directly with the managed device using CLI
To configure CLI console terminal preferences	To set user preferences for displaying of CLI text, logging CLI sessions text, and using CLI scripts in the Telnet or SSH console
To create and use CLI scripts	To create and use new or existing CLI scripts to manage modify device configurations
To save CLI scripts	To save newly-created or modified CLI scripts to a workstation directory or PC folder for storage or future use

12.5 CLI procedures

The following procedures describe how to launch and use the CLI.

Procedure 12-1 To launch a CLI session

- 1 You can:
 - a Use the navigation tree.
 - i Click on the Equipment tab.
 - ii Right-click on the device icon.
 - iii Choose CLI→*option* from the contextual menu, where *option* is Telnet Session or SSH Session.

The Telnet Session or SSH Session form appears for the device.

- b** Use the 5620 SAM main menu.
 - i** Choose Options→SR CLI→*option* from the menu, where *option* is Telnet Session or SSH Session.

The Telnet Session or SSH Session form appears.
 - ii** Type the management IP address of the device that you want to connect to beside the dimmed Connect button.
 - iii** Click on the Connect button.
 - 2** Log in using the required login user name and password.

You can now navigate the CLI according to your account security permissions.
-

Procedure 12-2 To configure CLI console terminal preferences

- 1** Launch a CLI session, as described in Procedure 12-1.
- 2** Right-click on the CLI console.

The CLI console contextual menu appears.
- 3** Choose Configure from the contextual menu.

The Terminal Configuration form appears.
- 4** Configure the parameters, as required.
 - i** Set the Minimum number of scrolling lines parameter to specify how many lines you can scroll and view before the lines are wrapped.
 - ii** Set the Font and Colors parameters to your viewing preferences.
 - iii** Select the Send Console To a File check box to send the console text to a log file.

When you choose to send the console output to a log file, you can specify the location of the log file using the Log File Location parameter.

 - Click on the Change button.

The Open form appears.
 - Navigate through the networkstation directory or PC folder structure for a log file storage location.
 - Enter a name for the log file or use cli_output.txt, which is the default name.
 - iv** Select the Show Scripting Command Buttons to enable CLI scripting functionality.
- 5** Click on the OK button to save the changes.

The Telnet or SSH session uses the new parameter settings.

Procedure 12-3 To create and use CLI scripts

CLI scripts are used to create a series of CLI commands on a particular managed device, then use a single button to execute the commands. This eliminates the need to type a long series of CLI strings. You can create CLI scripts that perform a function or functions and then run the scripts using command buttons in the Telnet or SSH command console.



Caution — CLI scripts that are not applied or created correctly can cause serious damage to your network. Alcatel recommends that system administrators clearly define user responsibilities for CLI script usage, and that scripts are verified and validated before they are performed on devices in a live network.

- 1 Launch a CLI session, as described in Procedure 12-1.
- 2 Select the Show Scripting Command Buttons to enable CLI scripting functionality.
- 3 Click on the OK button.

The Sample Command button appears in the Telnet or SSH console.

- 4 Right-click on the Sample Command button.

The sample command contextual menu appears.

- 5 Perform the required CLI script creation or management task from the appropriate contextual menu option.

- a Choose Add Command to add a CLI command script.

The CLI Scripting Command Configuration form appears.

- i Set the Name parameter to specify a name for the CLI script.
- ii Create a CLI script that includes the CLI commands you want to execute in the Script Definition panel. Use the sample CLI script as a guideline.

You can:

- create send requests that perform a function on the managed device and then send the output to the console
- create requests that perform an action using CLI commands described in the appropriate device reference guide, for example, the *7750 SR OS System Guide*

- iii Click on the OK button.

A command button, similar to the Sample Command button, is created in the Telnet or SSH console form.

- b Choose Configure Command to modify an existing CLI command script.

The CLI Scripting Command Configuration form appears with the name of the script in the Name parameter.

i Modify the existing CLI script, as required.

ii Click on the OK button.

The script is updated.

c Choose Move Button to change the position of a command button.

The button is highlighted in red.

i Select the button.

ii Move the button along the gray bar at the bottom of the console to its new location.

iii Drop the button.

The button appears in the new location.

d Choose Remove Command to remove the CLI script for the selected button.

The command button is removed.

e Choose Remove All Commands to remove all CLI scripts.

All command buttons, except the default Sample Command button, are removed.

f Choose Cancel to stop any action being performed in this step, or to stop a CLI command.

6 If you created or modified a CLI script:

i Click on the CLI command button to perform the command.

The CLI command is executed in the console

While the command is executed, an LED appears in the CLI command button. You can right-click on the button and choose Cancel from the contextual menu to stop the command.

ii Perform Procedure 12-4 to save the new or modified CLI script.



Caution — CLI scripts that are not applied or created correctly can cause serious damage to your network. Alcatel recommends that system administrators clearly define user responsibilities for CLI script usage, and that scripts are verified and validated before they are performed on devices in a live network.

Procedure 12-4 To save CLI scripts

- 1 Create or modify a CLI script, as described in Procedure 12-3.
- 2 Right-click on the script command button and choose Configure Command from the contextual menu.

The CLI Scripting Command Configuration form appears.

- 3 Click on the Save Script to File button.

The Open form appears.

- 4 Navigate through the workstation directory or PC file structure to locate a directory in which to store the script file.

- 5 Name the file appropriately with a .txt extension.

- 6 Click on the OK button.

The script file is saved.



Note — Alcatel recommends that you back up scripts to a secure location. This prevents the accidental loss of scripts by, for example, overwriting a script.

Router and IP/MPLS network configuration and management

- 13 — Equipment management overview**
- 14 — Equipment management using the navigation tree**
- 15 — Equipment management using the equipment manager**
- 16 — Router configuration**
- 17 — Routing protocol configuration**
- 18 — MPLS**
- 19 — Service tunnels**

13 — Equipment management overview

- 13.1 Equipment management overview 13-2**
- 13.2 Working with objects 13-3**
- 13.3 Working with network objects 13-4**
- 13.4 Working with device objects 13-5**
- 13.5 Working with LAG objects 13-7**
- 13.6 Working with shelf objects 13-8**
- 13.7 Working with card and card slot objects 13-8**
- 13.8 Working with daughter card objects 13-9**
- 13.9 Working with port and channel objects 13-10**

13.1 Equipment management overview

This chapter covers general equipment management information. The 5620 SAM equipment management interface consists of:

- a main menu
- contextual menus
- a navigation tree
- managed objects
- an equipment manager
- property forms to configure object parameters

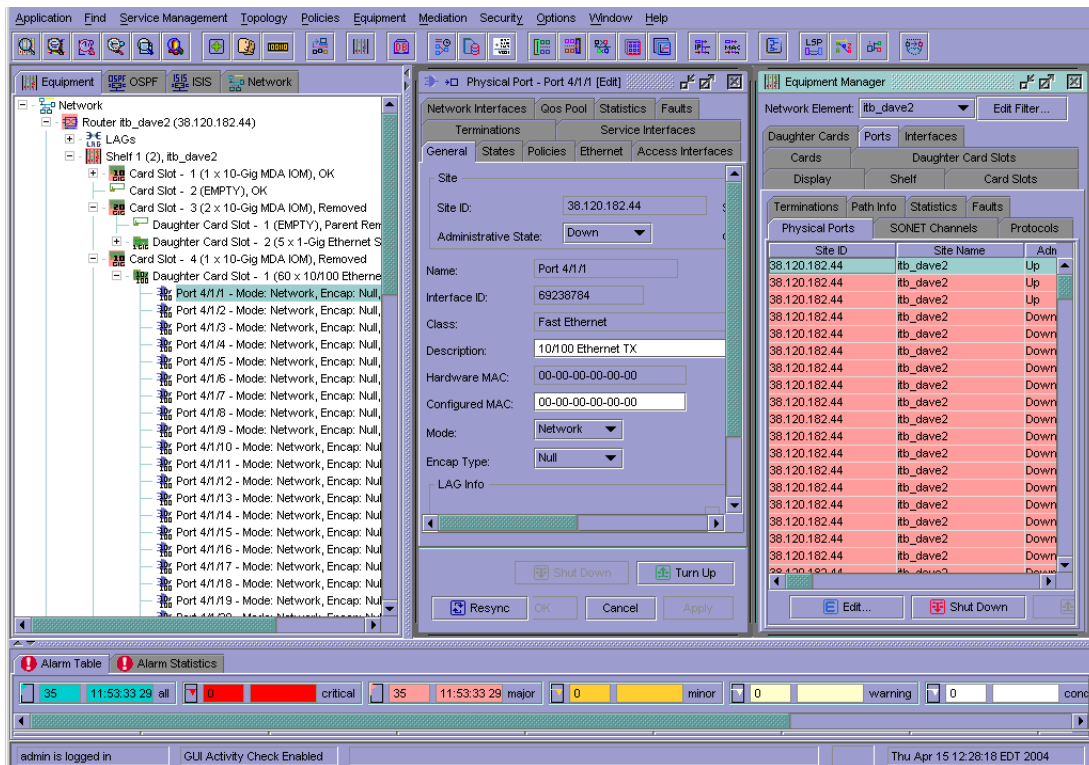
The 5620 SAM is used to create, configure, and manage a device with the various children objects required to be part of a network. Equipment such as the routers, which are at the top of the hierarchy, have properties that are configured using the CLI and discovered when the 5620 SAM discovery process is run.

After the device is discovered, you use properties forms to configure specific parameters for the child objects of the discovered device. The properties forms are opened from the contextual menus available for each created object under the Equipment tab in the navigation tree or from the equipment manager display tab after you choose an object and click an Edit button, a Create button, or when you double-click an object.

Figure 13-1 shows the 5620 SAM GUI used to manage equipment.

- The navigation tree on the left side has the Equipment tab selected and a daughter card from shelf 1, and card slot 4 is expanded to show the available ports.
- The equipment manager form on the right side displays the shelf and associated equipment parameters for the managed device under various tabs.
- The physical port configuration form is open for port 4/1/1 on the left side of the working pane. The form displays parameter information under each tab that can be configured for the managed equipment from the General tab.

Figure 13-1 GUI with equipment management drawings and forms



The 5620 SAM allows you to create and manage the following objects under the Equipment tab in the navigation tree:

- router or device — the highest level in the hierarchy
- LAG and shelf — each is at the second highest level in the hierarchy
- card — the highest level under the shelf, considered the parent object
- daughter card — a child object of the card object
- port — automatically created under each daughter-card, a child object of the daughter card
- channel — a child object of the port

13.2 Working with objects

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 tab and in the forms of the equipment manager.

The network is the top object in the navigation tree. 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.

- LAG
- shelf
- card slot
- card slot A for the CPM and switch fabric
- card slot B for the redundant CPM and switch fabric

The following objects must be created using property forms or create forms available from the contextual menus of the Equipment tab or the equipment manager.

- individual LAGs with LAG members
- cards
- 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. The following procedure is used to create objects using the navigation tree.

Procedure 13-1 To create an object

- 1 Right-click on an empty object in the navigation tree or in the Display tab of the equipment manager to open the contextual menu.
 - 2 Choose Properties or, when available, Create *<objectname>*.
The properties form or the create form, as applicable, appears.
 - 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 or equipment manager forms.
-

13.3 Working with network objects

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.

You can use the contextual menu option Create Group to group device icons. See chapter 14 for more information.

13.4 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 of the properties form and include the following:

- General
- Polling
- Protocols
- Faults

The following devices are supported:

- 7750 SR
- 7450 ESS

7750 SR support

The 7750 SR is an IP/MPLS service router designed to support the delivery of advanced Internet and VPN services

5620 SAM management of the 7750 SR provides element and network management functions. Table 13-1 lists the supported functions:

Table 13-1 7750 SR management

Functional area	Supported	Special information
Summary of functionality		
Full FCAPS support	✓	The 5620 SAM was designed to support the 7750 SR.
5620 SAM client GUI main menu		
Application→Exit	✓	—
Find→ <i>Submenus</i>	✓	—
Service Management→ <i>Submenus</i>	✓	All services are supported.
Topology→ <i>Submenus</i>	✓	—
Policies→ <i>Submenus</i>	✓	—
Equipment→Equipment Manager	✓	—
Mediation→ <i>Submenus</i>	✓	—
Security→ <i>Submenus</i>	✓	—
Options→ <i>Submenus</i>	✓	—
Window→ <i>Submenus</i>	✓	—
Help→ <i>Submenus</i>	✓	—
5620 SAM client GUI navigation tree		

(1 of 2)

Functional area	Supported	Special information
Equipment	✓	—
OSPF	✓	—
ISIS	✓	—
Network	✓	—

(2 of 2)

7450 ESS support

The 7450 ESS supports metro Ethernet and service-aware Ethernet aggregation across IP/MPLS networks.

5620 SAM management of the 7450 ESS provides element and network management functions. When a function or feature is not supported by the 7450 ESS, the feature or function cannot be selected from the GUI, or does not appear on the GUI.

Table 13-2 lists the supported functions:

Table 13-2 7450 ESS management

Functional area	Supported	Special information
Summary of functionality		
Releases	✓	Release 1.0 MIBs and functionality of the one-slot and seven-slot versions
Equipment management	✓	Supported in a similar fashion to 7750 SRs, with an additional Ethernet port parameter to enable oversubscription of the port
Spanning tree protocols	✓	Supported multiple types of spanning tree protocols, compliant with IEEE 802.d-2004, IEEE 802.1w, and backwards compatibility with dot1.w
Oversubscribed daughter card ports	✓	Additional statistics for ports to indicate how many packets or octets are dropped because the daughter card port is oversubscribed
MAC addressing for VPLS	✓	—
Unsupported functionality		
Global cflowd configuration and collection	—	Can specify IP interface, filter, and SAP statistics collection. When you configure the ACL IP filter policy, the cflowd-related parameters are not distributed to 7450 ESSs.
BGP	—	—
VPRN service	—	—
5620 SAM client GUI main menu		
Application→Exit	✓	—
Find→Submenus	✓	—

(1 of 2)

Functional area	Supported	Special information
Service Management→ <i>Submenus</i>	✓	The VPRN service is not configurable for 7450 ESSs. There are different configurations available for VPLS creation when a VPLS site is a 7450 ESS. <ul style="list-style-type: none"> three additional spanning tree protocol options and hold count values for BPDUs on the site forwarding tab edge-related parameters on the SAP and spoke SDP forwarding tab clear spanning tree protocol detected for specific encapsulation values on the SAP and spoke SDP forwarding tab
Topology→ <i>Submenus</i>	✓	—
Policies→ <i>Submenus</i>	✓	—
Equipment→Equipment Manager	✓	Shelf drawings are displayed for the one- and seven-slot versions.
Mediation→ <i>Submenus</i>	✓	Poller manager MIB entry tables have been modified to indicate the type of device and the release version of the MIB.
Security→ <i>Submenus</i>	✓	—
Options→ <i>Submenus</i>	✓	—
Window→ <i>Submenus</i>	✓	—
Help→ <i>Submenus</i>	✓	The number of supported cards is indicated in the license.
5620 SAM client GUI navigation tree		
Equipment	✓	Supports the 20G I/O module
OSPF	✓	—
ISIS	✓	—
Network	✓	BGP is not supported.

(2 of 2)

13.5 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 the LAG ID, Description, Configured address, Encap Type, and Administrative state
- LAG parameters such as Port threshold, Port Threshold Action, and Dynamic cost
- LACP such as the Administrative state, LACP Mode, LACP Transmit Interval, and the Actor Administration key
- 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. Only ports configured in network mode can belong to LAGs.

Up to 8 ports can be added or removed from the LAG. All ports added to a LAG must have the same parameter settings.

13.6 Working with shelf objects

Shelf objects represent the hardware that is configured in the router 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
- statistics
- faults

13.7 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 become visible in the navigation tree. They appear as empty card slots if a card is not provisioned for the slot. If a card is provisioned for the slot, it will be identified. Choose Configure Card from the contextual menu of the object and assign a supported card type for the slot. The following card types can be assigned to the card slots:

- 1X10-Gig MDA IOM for one daughter card
- 2X10-Gig MDA IOM for two daughter cards
- 60x10/100 Ethernet for up to 60 fast Ethernet ports

A card type 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 particular 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.

13.8 Working with daughter card objects

After the card is created in the card slot you can create and configure the daughter card object 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. Choose Configure Daughter Card from the contextual menu of the object and assign a supported daughter card type for the slot.

Table 13-3 lists the supported daughter card types

Table 13-3 Supported daughter cards

Managed device	Ethernet	SONET/SDH	Channelized
7750 SR	<ul style="list-style-type: none"> 10/100 Ethernet with 60 ports 100FX Ethernet with 20 ports Gigabit Ethernet with 5- and 10-port configurations 10 Gigabit Ethernet with 1 port 	<ul style="list-style-type: none"> OC3 and 16-port configurations OC12 and 16 port configurations OC48 and 4-port configurations OC192 with 1 port 	<ul style="list-style-type: none"> 1x OC12 Deep Channel has one port channelized to the DS0 level 12xDS3 Deep Channel has 12 ports channelized to the DS0 level and can also be used for DS3 clear channel applications
7450 ESS	<ul style="list-style-type: none"> 10/100 Ethernet with 60 ports 10/100/1000 Ethernet with 20 ports 100FX Ethernet with 20 ports 20 Gb/s I/O module Gigabit Ethernet with 10- and 20-ports 10XGigabit Ethernet XFP with 2 ports LAN/WAN physical card 	<ul style="list-style-type: none"> OC3 and OC12 16-port configurations OC48 and 4-port configurations OC192 with 1 port 	—

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.

13.9 Working with port and channel objects

The types of ports available depend on the daughter cards that are configured in the chassis. Ethernet ports cannot be channelized. SONET and TDM ports can be channelized. The following types of ports are supported:

- Fast Ethernet (10/100/100 BASE-T)
- Gigabit Ethernet (1000BASE-T)
- 10 Gigabit Ethernet (10000BASE-T)
- 10 Gigabit Ethernet (10GBASE-T)
- OC3/STM1, OC12/STM4, OC48/STM16, and OC192/STM64 SONET/SDH
- channelized OC12 and DS3

The port syntax is card slot/daughtercard/port. For example, Port 1/1/1 represents port 1 of daughter card 1 in slot 1 for any service. 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 that port for the service you want it to provide. The properties vary depending on whether the port type is one of the Ethernet type ports, SONET/SDH ports, or TDM ports. Channel objects are created on SONET 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 or the equipment manager to configure port and channel parameters. You can configure ports as network or access.

- Network ports connect and pass network-facing traffic.
- Access ports connect and pass customer-facing traffic for which services are configured.

Network ports are used in the service provider transport or infrastructure network, such as an IP/MPLS-enabled backbone network. Network ports can be assigned IP addresses and act as an Layer 3 interface. When network ports act as an Layer 3 interface, they can pass IP traffic to other devices and communicate using routing protocols, such as MPLS and OSPF.

Access ports are associated with a SAP, a subscriber, and a service to provide connectivity services to the subscriber, for example, a VLL service. Access ports and channels are configured for encapsulation, to differentiate the service on the port or channel. After a port is configured for access, one or more services can be configured for that port. All channelized ports that are configured as endpoints must be configured as access mode. Those that are not endpoints cannot be configured.

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 STS1 sub-channel, for example, the DS3 channel is built on the STS1 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 equipment manager.

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.

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:

- STS3 to STS192 clear-channels
- DS3 clear channel
- DS0 groups
- ports

STS3 to STS192 clear channel

STS3 to STS192 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 OCx card. See “SONET STS1 channelization and 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 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

Only the DS0 group level can be used as a connection termination point for SONET STS1 sub-channels. Channelization on the 1xOC12 can be used to create up to 12 SONET STS1 sub-channels. Each of these STS1 channels can be used to create a DS3 frame on which you can build DS1 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 of them. For example, you may use DS0 1, 3, 5, and 9 only, or another combination. See “SONET STS1 channelization and SONET clear-channel applications” in this section for more information.

Only the DS0 group level can be used as an endpoint on the channelized 12xDS3 card. Channelization can be used on each DS3 port of this card to create independent TDM channels in the form of DS1 data channels that handle DS0 groups. As with SONET sub-channels, the DS0s of a DS0 group can be configured in any sequence and you do not need to use all of them. For example, you may use DS0 1, 3, 5, and 9 only, or another combination. See “TDM channelization and clear channel applications” 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.

An access Ethernet 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 class of port that will be part of the Ethernet connection. For example, the Ethernet port Class parameter options are Fast Ethernet, Gigabit Ethernet, or 10G Ethernet. You must also configure the Encap Type parameter from the General tab at the connection termination point. Ethernet access ports use:

- Dot1 Q — Supports multiple services on the port. The outer encapsulation ID used to distinguish 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 ID used to distinguish services is the VLAN ID in the IEEE 802.1Q header.
- Null — Supports a single service on the port.

Ethernet network ports use:

- Dot1 Q
- Null

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 7750 SR must handle MTU limitations at many service points. The physical (access and network) ports, service, and service tunnel MTU values must be individually defined.
- Identify the ports to be designated as network ports and the ports to be designated as access ports intended to carry service traffic.
- MTU values should not be modified frequently.
- 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 Ethernet port MTU parameter indirectly defines the largest physical packet that the port can transmit or 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 exceed the MTU are discarded.

The parameters specified for MTU configuration include the destination MAC address, source MAC address, Ethernet encapsulation type, length field, and the complete Ethernet payload.

You must configure the duplex parameter from the Ethernet tab if the port will 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 option depending on the speed of the Ethernet interface.

SONET STS1 channelization and SONET clear-channel applications

Ports on OCx cards are SONET clear channel applications or SONET sub-channel applications. For example, 16xOC3 is for a clear channel application; the 1xOC12 Deep Channel is used for a SONET sub-channel application.

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 x OC3 SFP card, 16 ports are created. On each of these ports, you can create one full channel.

SONET sub-channel applications allow you to create multiple STS1 channels on a port that can be configured to have multiple DS0 connection termination points. For example, the following list shows the channelization sequence:

- 1 One OC12 port is created when you create a channelized 1xOC12 Deep Channel card.
- 2 This port can be channelized into 12 SONET STS1 sub-channels from the four STS3s available on the port.
- 3 You can then configure each of these STS1s to carry a DS3 frame.

- 4 Each DS3 frame can be channelized into 28 independent DS1 data channels that must be created one at a time.
- 5 For SONET sub-channel configuration, you must choose the Channelization Type for the next lower-level channel as Channelized at the DS3 level. You must select Channelized DS1 as the Channel Type on the port to create the DS3 channel. Each DS1 channel can be configured to handle up to 24 DS0 groups. To use a DS1, you must create at least one DS0 group for the DS1.

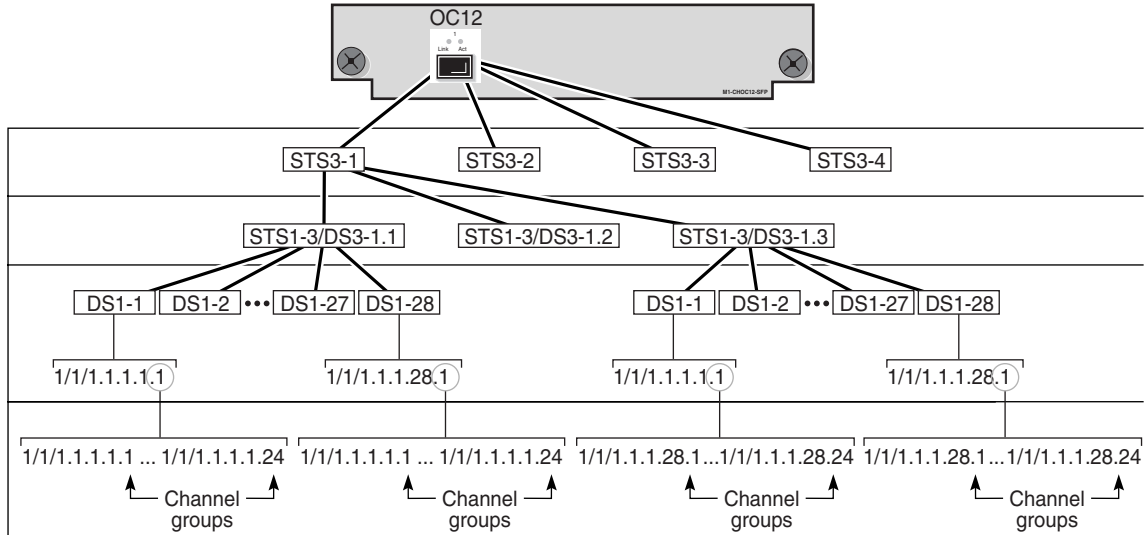
Table 13-4 lists the available channelization options for each application.

Table 13-4 Channel parameters

Applications	Channel ranges						
	STS192	STS48	STS3	STS1	DS3	DS1	DS0
SONET Clear channel	1	1	1		1		
SONET Sub channel			1 to 4	1 to 3	1	1 to 28	1 to 24
TDM					1	1 to 28	1 to 24

Figure 13-2 shows the channelized 1xOC12 port structure.

Figure 13-2 Channelized 1xOC-12 port structure



17455

Table 13-5 provides an example of the naming conventions for a channelized 1xOC12 port. The syntax for a SONET sub-channel is:

```
card slot/daughtercard/port.STS1-[STS3#].[STS1#]
```

For a DS3 channel from an STS1 sub-channel, the syntax is:

```
slot/daughtercard/port.DS3 [STS3#].[STS1#]
```

For a DS1 channel from a DS3 channel, the syntax is:

slot/daughtercard/port.DS1 [STS3#] . [STS1#] . [DS1#]

Table 13-5 Example of SONET sub-channel naming convention

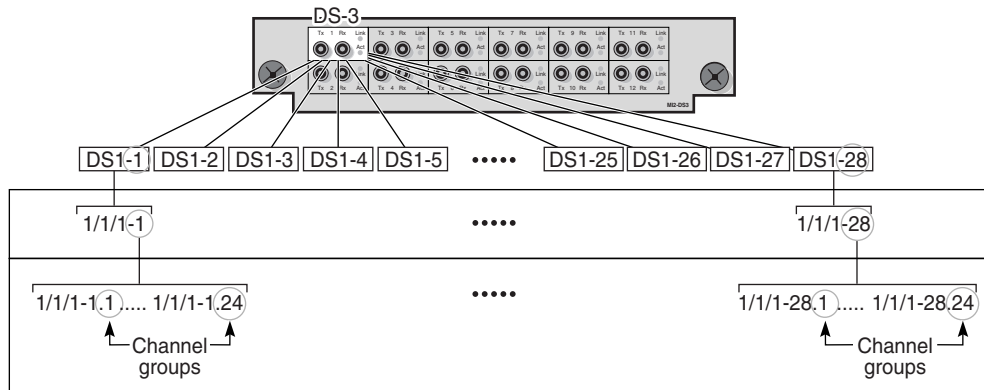
Syntax	Description	Notes
Channel 1/1/1.sts1-2.2	1/1/1 is the slot number/daughtercard number/port number 2 is the STS3 number (1 to 4) .2 is the STS1 number (1 to 3)	The sts1 parameter is 2.2 which means that it is the fifth STS1. There are four STS3s for an OC-12 and each STS3 has three STS1s such that the fifth STS1 is the second STS1 of the second STS3.
Channel 1/1/1.ds3 2.2	.ds3-2 is the STS3 number (1 to 4) .2 identifies the STS1 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.DS0Grp-2.2.25.5	.DS0Grp-2.2.25.5 identifies one of the DS0 channel groups (1 to 24) on the DS1	The DS0 is configured on the DS1 channel.

TDM channelization and clear channel applications

When you create a 12xDS3 card, 12 DS3 ports are created. Each DS3 channel can be channelized into 28 independent DS1 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. To use a DS1, you must create at least one DS0 group for the DS1.

By default, DS3 ports are automatically created for clear channel connections. To create a channelized DS3, you must configure the DS3 channel as TDM and Channelized before you create the DS1 channels for channelized TDM connections. To channelize the DS3 to the DS0 level, you must set the Channelization Type to Channelized DS1. Figure 13-3 shows the channelized DS3 port structure.

Figure 13-3 Channelized 12xDS3 port structure



17454

Table 13-6 provides an example of the naming conventions for a 12xDS3 port. The channel syntax for a TDM-based DS3 channel is:

```
card slot/daughtercard/port.DS3-
```

For a DS1 channel from a TDM-based DS3 channel, the syntax is:

```
slot/daughtercard/port.DS1-[STS3#].[STS1#].[DS1#]
```

For a DS0 group channel from the DS1 channel, the syntax is:

```
slot/daughtercard/port.DS0Grp-[STS3#].[STS1#].[DS1#].[Group#]
```

Table 13-6 Example of TDM channel naming convention

Syntax	Description	Notes
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.ds1-1.1.2	.ds1 identifies the channel as DS1 1 is the STS3 number (1 to 4) .1 is the STS1 number (1 to 3) .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.
Channel 1/1/1.ds0Grp-1.1.2.23	.ds0Grp- identifies the channel as a DS0 group 1 is the STS3 number (1 to 4) .1 is the STS1 number (1 to 3) .2 is the DS1 number (1 to 28) .23 identifies the DS0 channel group (1 to 24) on the DS1	The DS0 group is configured on the DS1 channel. Only a DS0 can be used as a CTP.

14 — Equipment management using the navigation tree

- 14.1 Navigation tree overview 14-2**
- 14.2 Workflow to manage equipment using the navigation tree 14-7**
- 14.3 Navigation tree menus 14-7**
- 14.4 Navigation tree procedures list 14-7**
- 14.5 Navigation tree procedures 14-8**

14.1 Navigation tree overview

The navigation tree Equipment tab button contains all the physical objects that the 5620 SAM manages and that can be created in a hierarchical order for the managed device. There can be more than one managed device object in the navigation tree. In the navigation tree, you can use the contextual menu choices to create, configure, and manage specific parameters for the children objects of the discovered device.

The 5620 SAM allows you to manage and create the following objects under the Equipment tab in the navigation tree:

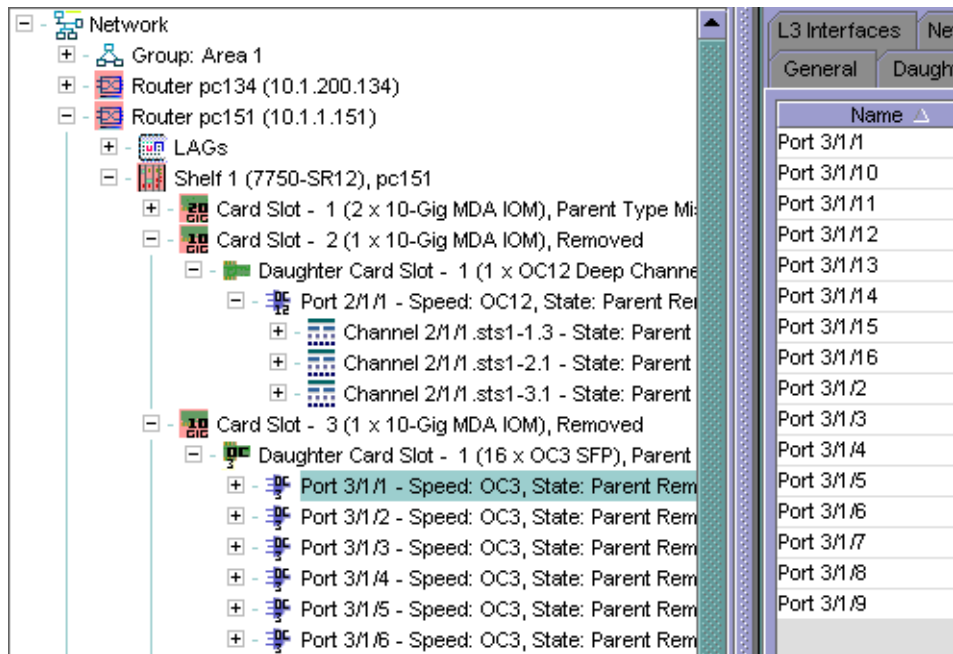
- network — containing all routers and devices
- group — to group devices together logically
- router and device — the next level in the hierarchy
- LAG and shelf — each is at the third highest level in the hierarchy
- card — the highest level under the shelf, considered the parent object
- daughter card — a child object of the card object
- port — automatically created under each daughter card, a child object of the daughter card
- channel — a child object of the port

To access objects in the navigation tree from the 5620 SAM:

- Click on an object under the Equipment tab in the navigation tree and use the + and - icons to navigate the hierarchy of network equipment objects, from the device to the ports and channels.
- Right-click on each object to open the contextual menu and choose a function. The functions available from the contextual menu are specific to each object in the hierarchy.

Figure 14-1 shows some of the navigation tree objects that you can view from the Equipment tab button.

Figure 14-1 Navigation tree objects - Equipment tab



Contextual menus for objects in the navigation tree

The contextual menus reside on each object and are a right-click function in both the navigation tree and the equipment manager Display tab. They are used to create objects, configure properties for objects, perform maintenance duties, change states on object parameters, and provide another management interface.

The following describes the contextual menu options available for each object in the navigation tree hierarchy:

- The contextual menu option for Network is Create Group, used to group routers and devices.
- The contextual menu options for a device includes:
 - Add to Group
The Add to Group menu option specifies whether to add the device to a group.
 - Resync
The Resync menu option specifies that MIB tables are re-read to resynchronize them with the 5620 SAM which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.
 - Equipment Manager
The equipment manager menu option on the contextual menu and on the main menu opens the equipment manager form for the router chosen in the Equipment tab of the navigation tree. The equipment manager form has eight tabs from which you can view and edit information.
 - CLI
The CLI option allows you to open a Telnet Session or an SSH Session with the device that has been chosen in the Equipment tab of the navigation tree.
 - Properties
The Properties option opens the property form for the chosen object. This form displays read-only information and configurable parameters.
- The contextual menu options for LAGs include:
 - Resync
The Resync menu option specifies that MIB tables are re-read to resynchronize them with the 5620 SAM which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.
 - Create LAG
The Create LAG option opens the Create LAG configuration form that allows you to create a link aggregation group. You define LAG properties, configure LAG parameters, configure LACP, and configure LAG members.
 - Properties
The Properties option opens the properties form where you configure LACP System priority parameter.
- The contextual menu options for a shelf include:
 - Resync
The Resync menu option specifies that MIB tables are re-read to resynchronize them with the 5620 SAM which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.
 - Reboot
The Reboot option specifies that all cards in the chassis are re-initialized.
 - Properties

The Properties option opens the properties form where you can view and edit properties contained in the shelf. You can view general properties for the shelf, such as fan trays, power supply trays, and LED panels, and view and change the properties for objects contained in the shelf, such as hardware environment, card slots, statistics policies, and faults.

- The contextual menu options for a card slot include:
 - Resync
The Resync menu option specifies that MIB tables are re-read to resynchronize them with the 5620 SAM which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.
 - 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 and Allowed Card Types parameters. The Equipped Card Type displays the card type that is physically in the slot. When there is a mismatch between the Equipped Card Type and the Assigned Card Type, a check mark appears in the Mismatch box. When the configured card types are correct, you can change the Administrative State as required.
 - Properties
The Properties option opens the properties form where you can view and change properties contained in the card slot. After the card object is created, you can use the properties option on the slot to view, edit, and create all the properties that can be contained in the card slot, for example daughter cards and ports.
 - Reboot
The Reboot option specifies that all cards in the chassis are re-initialized.
 - Shut Down
The Shut Down option specifies that the card slot is changed to administratively down.
 - Turn Up
The Turn Up option specifies that the card slot is changed to administratively up.
 - 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.
- The contextual menu options for a daughter card slot include:
 - Resync
The Resync menu option specifies that MIB tables are re-read 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.
 - Configure Daughter Card
The Configure Daughter Card option opens the Create Daughter Card properties 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 and Allowed Daughter Card Types areas of the form. The Equipped Daughter Card Type displays the daughter card type that is physically in the slot. When there is a mismatch between the Equipped Daughter Card Type and the Assigned Daughter Card Type, a check mark appears in the Mismatch box. When the configured card types are correct, you can change the Administrative State as required.

- Properties
The Properties option opens the properties form. You can view and change properties in the daughter card slot. After the daughter card object is created, you can use the properties option on the slot to view, modify, and create all the properties that can be contained in the slot, for example daughter cards and the QoS Pool for the daughter card slot.
- Reboot
The Reboot option specifies that all daughter card slots in the chassis are re-initialized.
- Shut Down
The Shut Down option specifies that the daughter card slot is changed to administratively down.
- Turn Up
The Turn Up option specifies that the daughter card slot is changed to administratively up.
- Remove
The Remove option deletes the daughter card from the slot when the slot and everything contained in the slot is changed to administratively down.
- The contextual menu options for ports include:
 - Resync
The Resync menu option specifies that MIB tables are re-read 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.
 - Properties
The Properties option opens the properties form. You can view and change properties contained in the port. Port objects are automatically created when the daughter card object is created. Use the properties option on the slot to view, change, and create all the properties that can be contained in the slot, for example, SONET channels.
 - Reboot
The Reboot option specifies that all ports are re-initialized.
 - Shut Down
The Shut Down option specifies that the port is changed to administratively down.
 - Turn Up
The Turn Up option specifies that the port is changed to administratively up.
 - Remove
The Remove option deletes the port when everything contained in the port is changed to administratively down.

14.2 Workflow to manage equipment using the navigation tree

- 1 Discover the device.
- 2 Right-click on the object in the navigation tree to open the contextual menu.
- 3 Choose an option. See section 14.1 for a list of contextual menu options.
- 4 Configure the parameters, as required.
 - i Edit the device parameters as required using the Properties form from the contextual menu.
 - ii Create card objects in the shelf using the Properties forms from the contextual menu in the Equipment tab.
 - iii Create daughter card objects in the card objects using the Properties forms from the contextual menu in the Equipment tab.
 - iv View the parameters of the port objects that were created automatically with the daughter card object using the Properties forms from the contextual menu in the Equipment tab.
 - v Edit the parameters of the created objects as required using the Properties forms from the contextual menu in the Equipment tab.
 - vi Create channel objects on the SONET/SDH and TDM ports using the Properties forms from the contextual menu in the Equipment tab.
 - vii Edit the channel parameters as required using the Properties forms from the contextual menu in the Equipment tab.
- 5 Save the configuration, as required.

14.3 Navigation tree menus

Table 14-1 lists the menu items to manage and configure equipment using the navigation tree.

Table 14-1 5620 SAM equipment management navigation tree menus

Menu option	Task
Contextual menu for Equipment tab objects in the navigation tree	View, open, create and configure properties or start a Telnet or SSH session.

14.4 Navigation tree procedures list

Table 14-2 lists the procedures to configure equipment using the navigation tree.

Table 14-2 5620 SAM equipment management using the navigation tree procedures list

Procedure	Purpose
To group devices and routers	Create and configure devices, including the router, chassis, slots, cards, daughter card slots, daughter cards, ports, channels, and LAGs.
To change device properties	
To create and configure a LAG	
To create a card type	
To create daughter cards	
To configure Ethernet ports	
To configure SONET ports	
To configure TDM ports	
To configure SONET clear channels and SONET STS1 sub-channels	
To configure TDM channels	
To delete network equipment	See the Cards and Ports chapter in the <i>7750 SR OS System Guide</i> for more information.

14.5 Navigation tree procedures

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

Procedure 14-1 To group devices and routers

You can use the grouping function to:

- represent devices that are located in the same geographical area
- indicate network topology, for example, grouping devices that operate in the same spanning tree or SONET/SDH ring

The following general rules apply to groups:

- managed devices, such as the 7750 SR and the 7450 ESS, can belong to multiple groups
- you cannot expand device icons within a group from the navigation tree, however, you can open properties for the device
- you can view only network element-level alarms from device icons within a group

- 1 Click on the Equipment tab in the navigation tree.
- 2 Right-click on the Network icon and choose Create Group from the contextual menu.

The Group (Create) form appears.

- 3 Specify the Group Name parameter. You cannot modify the Group Name parameter for a group once the group is created.

- 4 Provide a description of the group, for example, to indicate its geographical location or the spanning tree that the group represents.

- 5 Click on the OK button.

The Group:*name_of_group* icon appears in the navigation tree.

- 6 You can add devices to the group using the Group (Edit) form or add devices from the device icon.

- a To add devices to a group using the Group (Edit) form.

- i Click on the Group:*name_of_group* icon in the navigation tree.

- ii Choose Properties from the contextual menu.

The Group (Edit) form appears.

- iii Click on the Group Members tab button.

- iv Click on the Add button.

The Select Network Elements form appears.

- v Choose a device or devices from the list and click on the OK button.

The device or devices are added to the group member list.

- vi Open the Group:*name_of_group* icon.

The device or device icons appears.



Note — You cannot expand the device using the device icon within the group.

- b To add devices to the group using the device icon.

- i Click on the device icon that you want to belong to a group.

- ii Choose Add to Group from the contextual menu.

The Select Group form appears.

- iii Select a group from the list and click on the OK button.

- iv Open the Group:*name_of_group* icon.

The device appears.



Note — You cannot open the device using the device icon within the group.

- 7 You can administrate groups as required.

- a To remove a device from a group, select the device icon within the Group:*name_of_group* icon and choose Remove From Group from the contextual menu.

The device is removed.

- b To remove a group, select the Group:*name_of_group* icon and choose Remove Group from the contextual menu.

Verify the action.

The group is removed from the navigation tree.

- c To view network-level alarms from a device within a group, click on the Faults tab.
-

Procedure 14-2 To change device properties

- 1 Right-click on a discovered device in the navigation tree and choose Properties from the contextual menu.

The properties forms for the device is displayed.

- 2 View and modify the parameters, as required. For example, you can configure supported protocols using the Protocols tab. See chapter 17 for more information about configuring protocols.

- 3 View groups that this device belongs to. See Procedure 14-1 for more information.
-

Procedure 14-3 To create and configure a LAG

- 1 Right-click on the LAG object in the navigation tree and choose Create LAG from the contextual menu

The Create LAG form appears.

- 2 Follow the steps to configure the LAG parameters.

Figure 14-2 shows the Create LAG form at the Define General Properties step.

Figure 14-2 Create LAG form - Define General Properties step

The screenshot shows a web-based configuration window titled "Create LAG - LAG". The main area is titled "Define General Properties". On the left, a "Steps" sidebar lists four steps: "1. Define General Properties" (highlighted), "2. Configure LAG Parameters", "3. Configure LACP", and "4. Configure LAG Members". The main form contains the following fields:

- LAG ID: Auto-Assign ID
- Description:
- Configured Address:
- Encap Type:
- Port Class:

At the bottom of the form are four buttons: "< Back", "Next >", "Finish", and "Cancel".

- 3 Define the General properties.
 - i Configure or auto-assign the LAG ID.

The LAG ID identifies the LAG in the database and creates the context for configuring LAG parameters.
 - ii Configure the description.
 - iii Configure the MAC address of the LAG.
 - iv Configure the Encap Type parameter as Null or Dot1 Q
 - v Configure the Administrative State.
 - vi Click on the Next button.
- 4 Configure LAG parameters.
 - i Set the Port Threshold and Port Threshold Action parameters to specify the behavior for the LAG if the number of operational links falls below the configured threshold level.
 - ii Set the LAG Dynamic Costing parameter. Dynamic costing can be turned on or off using the check box button.
 - iii Click on the Next button.
- 5 Configure LACP.
 - i Enable or disable the LACP by selecting or deselecting the Administrative State check box.

When you enable LACP, you can configure the following parameters.

- LACP Mode to active or passive
 - Actor Administration Key value
 - LACP Transmit Interval to slow or fast
- ii Set the LACP Mode to specify whether the LACP is active or passive. One end of the LAG group must be configured as active for LACP to work properly.
 - iii Set the Actor Administration Key value to uniquely identify the LACP.
 - iv Set the LACP Transmit Interval to specify whether transmissions are slow or fast.
 - v Click on the Next button.
- 6** Configure LAG Members.

- i Click on the Add button from the configure LAG members configuration to add network ports to LAGs.

The Create LAG member series of configuration steps appears.

- ii Click on Show only Compatible Ports and ensure the correct class of service is configured.
- iii Click on the Next button.
- iv Select compatible ports from the list to construct the LAG.

Add ports to an LAG as follows:

- Choose up to eight ports from the list of ports.
- Click on the Next button.
- Define the priority of the LAG.
- Click on the Finish button.



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 Edit 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.

- 7 Use the Properties contextual menu to view information about the created LAG, or modify LAG parameters.
 - The General tab displays the LAG ID, the description, and the 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.
 - Statistics, terminations, and fault information is available from the appropriate tabs.
-

Procedure 14-4 To create a card type

- 1 Choose Configure Card from the contextual menu on any one of the empty Card Slot objects in the navigation tree.

The Card Slot (Create) configuration form appears.

The number of slots depends on how many configured cards there are, and how many slots are on the managed router. Empty slots and configured slots are listed.

- 2 Choose the card type for the Assigned Card Type parameter. The options are:
 - 1X10-Gig MDA IOM for one daughter card
 - 2X10-Gig MDA IOM for two daughter cards
- 3 Click on the OK button to save the changes.

The card and slot appear in the navigation tree and in the inventory list of the equipment manager.

Procedure 14-5 To create daughter cards

- 1 Choose Configure Daughter Card from the contextual menu on a Card Slot object in the navigation tree. Different cards can have different numbers of daughter card slots, some have one daughter card slot and some have two daughter card slots. If there is a plus sign beside the Card object, click on it to expand the tree then choose a daughter card slot for the daughter card.

The Daughter Card Slot (Create) configuration form appears.

- 2 Choose the daughter card type for the Assigned Daughter Card Type parameter. The options that appear depend on the type of device and include the following:

- 60 x 10/100 Ethernet
- 10 x 1-Gig Ethernet SFP
- 16 x OC12/OC3 SFP
- 8 x OC12/OC3 SFP
- 16 x OC3 SFP
- 8 x OC3 SFP
- 4 x OC48 SFP
- 1 x OC192
- 5 x 1-Gig Ethernet SFP
- 12 x Ds3 Deep Channel
- 1 x OC12 Deep Channel
- 1 x 10-Gig Ethernet
- 4 x OC3 Deep Channel
- 2 x OC48 SFP
- 20 x 10/100 Ethernet Fx
- 20 x 10/100/1000 Ethernet Tx
- 20 x 10/100/1000 Ethernet SFP
- 2 x 10-Gig Ethernet XFP

- 3 Click on the QoS Pool tab button.
- 4 Choose a QoS pool from the available list of QoS policies, such as network ingress and access ingress.
- 5 Click on the OK button.

The daughter card and all its ports appear in the navigation tree and in the inventory list of the equipment manager.

Procedure 14-6 To configure Ethernet ports

Perform the steps in this procedure as required depending on the daughter card and port type that you are configuring.

- 1 Right-click on the port object in the navigation tree and choose Properties from the contextual menu

The properties form appears.
- 2 Configure port parameters as appropriate. Figure 14-3 shows the port configuration form for an Ethernet port with the General tab selected.

Figure 14-3 Ethernet port configuration form - General

Physical Port - Port 1/1/16, 10.1.200.51 [Edit]

General States Ethernet Terminations L2 Interfaces L3 Interfaces Qos Pool Statistics Faults

Site

Site ID: 10.1.200.51 Site Name: sim200.51

Name: Port 1/1/16 CLI Name: 1/1/16

Interface ID: 19398656

Class: Fast Ethernet

Description: 10/100 Ethernet TX

Hardware MAC: 90-33-01-01-00-10

Configured MAC: 90-33-01-01-00-10

Mode: Access

Encap Type: Null

Speed: 100

Actual Speed (KBytes): 0

MTU (bytes): 1514

Hold Time

Hold Time Up: 0 Hold Time Down: 0

Resync Shut Down Turn Up Reset OK Cancel Apply

i Configure the Mode parameter. The options are:

- Access
- Network

An access port is used for customer-facing traffic on which services are configured. SAPs can only use an access port or channel. When a port is configured for access mode, the appropriate encapsulation type must be specified to distinguish the services on the port. The appropriate Encap Type can be configured on the terminating port.

A network port or channel configured for network access participates in the service provider transport or infrastructure network. When the network option is configured, the encapsulation type cannot be configured. When network ports are configured, the appropriate control protocols are activated when necessary.

ii Configure the Encap Type parameter from the General tab.

For Ethernet access ports, the options are:

- Dot1 Q — Supports multiple services on the port. The outer encapsulation ID used to distinguish 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 ID used to distinguish services is the VLAN ID in the IEEE 802.1Q header.
- Null — Supports a single service on the port.

For Ethernet network ports, the options are:

- Dot1 Q
- Null

- iii Configure MAC addresses using the configured address parameter for ports and LAGs from the General tab.

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.

- iv Click on the Policies tab to configure parameters that are related to access and network buffering policies.

- To change the network queue policy from the Policy tab, click on the Select button.
- Click on a policy from the Bind list and click on the OK button to bind the port to a policy.
You can modify the network queue policy configuration using the Edit button, or you can pre-set network queue policies as described in chapter 20.

Click on the QoS Pool tab to view egress, ingress, and buffer policies in effect on the port. Click on a policy in the list, then click on the Edit button to view additional information about the settings, such as the CBS rate and the slope policy in effect.

- v Specify the MTU size for an Ethernet port using the MTU (bytes) parameter on the General tab.

Table 14-3 lists the default MTU values for network and access ports.

Table 14-3 Default MTU values for ports

Port type	Port/channel mode configuration	Encapsulation type	Default MTU size (Bytes)
Ethernet	Access	null	1514
Ethernet	Access	dot1q	1518
Fast Ethernet	Network	n/a	1514
Other Ethernet	Network	n/a	9212

Consider the following when you configure MTU parameters:

- The 7750 SR must handle MTU limitations at many service points. The physical (access and network) ports, service, and service tunnel MTU values must be individually defined.
- Identify the ports to be designated as network ports and the ports to be designated as access ports intended to carry service traffic.
- MTU values should not be modified frequently.
- 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 Ethernet port-level MTU parameter indirectly defines the largest physical packet that the port can transmit or 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 exceed the MTU are discarded.

The parameters specified for MTU configuration include the destination MAC address, source MAC address, Ethernet encapsulation type, length field, and the complete Ethernet payload. A major divergence between channel and Ethernet physical MTU values is in what overhead is considered part of the framing method and what overhead is considered to be part of the application using the frame.

- vi** Configure the duplex parameter from the Ethernet tab, if required. Use the full duplex option if the port will be added to a LAG.
- vii** Configure the Dot1 Q Ethertype and Q in Q Ethertype parameters from the Ethernet tab, if required. The range is 1536 to 65 535.
- viii** Configure the Ingress Rate parameter for Ethernet ports on 7450 ESSs. The range is -1 (default) to 10000. Use the parameter to specify oversubscribing for the selected port.
- ix** Configure the speed parameter if available, from the General tab. The options are:
 - 10
 - 100
 - 1000
 - 10000

The options that are available depend on the speed of the Ethernet interface

- 3** You can review port statistics from the port configuration form. Figure 14-4 shows a sample list of statistical counters from a port from the Statistics tab.

Figure 14-4 Sample statistics list - Statistics

Record Type	Update	Suspect	Time Captured	History Created	Periodic Time	Monitored Obj
Non-Scheduled Select...	Scheduled Full	<input type="checkbox"/>	08/26/2004 11:09:23 5...	<input type="checkbox"/>	5392245	network:38.120.1
Scheduled Full	Scheduled Full	<input type="checkbox"/>	08/26/2004 11:09:23 5...	<input checked="" type="checkbox"/>	5392261	network:38.120.1

Procedure 14-7 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 Right-click on the port object in the navigation tree and choose Properties from the contextual menu.

The properties form appears.

- 2 Configure port parameters as appropriate. Figure 14-5 shows the port configuration form for a SONET port with the General tab selected.

Figure 14-5 SONET port configuration form - General

Physical Port - Port 10/1/1, 10.1.1.18 [Edit]

SONET Overhead | L2 Interfaces | L3 Interfaces | Network Interfaces | Qos Pool | Statistics | Faults

General | States | Channels | SONET | SONET Monitoring

Site

Site ID: 10.1.1.18 Site Name: pc18

Name: Port 10/1/1 CLI Name: 10/1/1

Interface ID: 169902080

Class: SONET

Description: OC-12 SONET/SDH

Speed: OC12

Resync Shut Down Turn Up Reset OK Cancel Apply

i Configure the Mode parameter from the General tab. The options are:

- Access
- Network

An access port or channel is used for customer-facing traffic on which services are configured. SAPs can only use an access port or channel. When a port is configured for access mode, the appropriate encapsulation type must be specified to distinguish the services on the port or channel. The appropriate Encap Type must be configured on the terminating channel. For example, if the DS3 channel is the connection termination endpoint, the Encap Type can be configured on the General tab. After a channel is configured for access mode, multiple services can be configured on the port.

A network port or channel configured for network access participates in the service provider transport or infrastructure network. When the network option is configured, the encapsulation type cannot be configured.

When network ports are configured, the appropriate control protocols are activated when necessary. For example, configuring an IP interface on the SONET/SDH channel activates IPCP, while the removal of the IP interface causes the IPCP to be removed. The same applies for other routing protocols, such as MPLS.

ii Configure the Encap Type parameter from the General tab at the connection termination point.

For SONET or SDH, access ports or channels, the options are:

- BCP Null — Supports a single service on the POS port or channel. This is used to bridge a service between two devices using PPP over SONET/SDH or TDM. The encapsulation ID is always 0.
- IPCP — Supports one IP service on the port or channel. This is typically used for device interconnection using PPP.
- BCP Dot1 Q — Supports multiple services on the port or channel. This encapsulation type is used to bridge multiple services between two devices using PPP over SONET/SDH or TDM. The outer encapsulation ID, which is used to distinguish services, is the VLAN ID in the IEEE 802.1Q header in the BCP-encapsulated frame.
- FR — Supports multiple services using the DLCI header.

For SONET/SDH network ports, the only option is PPP Auto.

- iii Configure MAC addresses using the configured address parameter for ports or BCP-enabled SONET channels from the General tab.

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.

- iv Click on the Policies tab or QoS Pools tab to configure parameters that are related to access and network buffering policies.
 - To change the network queue policy, click on the Select button.
 - Click on a policy from the Bind list and click on the OK button to bind the port to a policy.
You can modify the network queue policy configuration using the Edit button, or you can pre-set network queue policies as described in chapter 20.

Click on the QoS Pool tab to view egress, ingress, and buffer policies in effect on the port. Click on a policy in the list, then click on the Edit button to view additional information about the settings, such as the CBS rate and the slope policy in effect.

- v Specify the MTU size for a SONET/SDH channel using the MTU (bytes) parameter on the General tab at the connection termination endpoint.

Table 14-4 lists the default MTU values for network and access ports.

Table 14-4 Default MTU values for ports

Port type	Port/channel mode configuration	Encapsulation type	Default MTU size (bytes)
SONET/SDH clear-channel	Access	bcp null	1522
SONET/SDH clear-channel	Access	bcp dot1q	1526

(1 of 2)

Port type	Port/channel mode configuration	Encapsulation type	Default MTU size (bytes)
SONET/SDH clear-channel	Access	ipcp	1502
SONET/SDH	Network	n/a	9208

(2 of 2)

The parameters specified for MTU configuration include the destination MAC address, source MAC address, Ethernet encapsulation type, length field, and the complete Ethernet payload. SONET channels use the MTU value to define the largest point-to-point payload that a SONET frame may contain. A major divergence between channel and Ethernet physical MTU values is in what overhead is considered part of the framing method and what overhead is considered to be part of the application using the frame.

- vi** Configure the speed parameter, if available, from the General tab. The options are:
 - Line Rate
 - OC3
 - OC12
 - OC48
 - OC192

- vii** Configure the SONET/SDH port parameters to define how the port operates.
 - Specify whether to use SONET or SDH.
 - Specify the speed of the port, from OC3/STM1, depending on the card type.
 - Specify an internal (node timed) or lined (looped-timed) clocking source for SONET.
 - Specify a loopback mechanism for SONET: Line, Internal, Remote, or None.

- viii** Configure the SONET/SDH channel parameters to define how the channel operates.
 - Specify the administrative state as Up from the States tab.
 - Specify the control packet header and payload parameters from the Channel Overhead Monitor, Channel, or SONET Overhead tabs.
 - Choose 16- or 32-bit cyclic redundancy checking (CRC).
 - Enter a J0 string that identifies the circuit. This string is inserted continuously at source. This can be checked against the expected value by the receiver. If no string is entered, then a null string is used.
 - Enter a C2 byte value that communicates the payload type being encapsulated by SONET framing.
 - Choose a SONET section trace mode from the list.
 - Specify the keepalive settings from the PPP tab, if required.
 - Set the keepalive period to specify the interval, in seconds, that echo requests are issued.
 - Set the drop count interval to specify how many keepalive messages are missed before the line is brought down.
 - Set the Link quality messages (LQMs) parameter to replace keepalive messages and provide link quality report data.

- ix** Configure the alarm reporting parameters for the SONET/SDH frames from the Channel Monitoring tab.
 - Specify the BER threshold information.
 - Specify the types of alarms to be reported for the SONET/SDH port, for example, Tx and Rx errors, and framing errors.

- x Configure the SONET/SDH sub-channel from the SONET Sub-channel tab as appropriate.
 - Choose a channel from the list and click on the Edit button to view the channel parameters.
 - 3 You can review port statistics from the port configuration form.
-

Procedure 14-8 To configure TDM ports

Perform the steps in this procedure as required depending on the port type that you are configuring.

- 1 Right-click on the port object in the navigation tree and choose Properties from the contextual menu.

The properties form appears.
- 2 Configure port parameters as appropriate. Figure 14-6 shows the port configuration form for a TDM port with the General tab selected.

Figure 14-6 TDM port configuration form - General

The screenshot shows a web-based configuration interface for a TDM port. The title bar reads 'Physical Port - Port 10/2/1, 10.1.1.18 [Edit]'. Below the title bar are several tabs: 'General', 'States', 'Policies', 'Channels', 'DS3E3', 'Qos Pool', 'Statistics', and 'Faults'. The 'General' tab is active. The form contains the following fields and controls:

- Site:** Site ID: 10.1.1.18, Site Name: pc18
- Name:** Port 10/2/1, CLI Name: 10/2/1
- Interface ID:** 171999232
- Class:** TDM
- Description:** DS3E3
- Speed:** Line Rate (dropdown menu)

At the bottom of the form, there are several buttons: 'Resync', 'Shut Down', 'Turn Up', 'Reset', 'OK', 'Cancel', and 'Apply'.

- i Configure a meaningful description for the port that makes it easily identifiable.
 - ii Configure the Administrative State as up or down on the States tab.
 - iii Configure the Line Buildout for TDM as short or long as necessary.
 - iv Click on the QoS Pool tab, as required, to configure parameters that are related to buffering policies.
 - To change the Slope policy from the QoS Pool tab, click on the Select button.
 - Bind the port to a policy from the list by clicking on a policy from the list and click on the OK button.

You can modify the Slope policy configuration using the Edit button and pre-setting the policies as described in chapter 20.
 - Configure the percentage of Reserved CBS using the sliding scale or choose the default value.
- 3 You can review port statistics from the port configuration form.

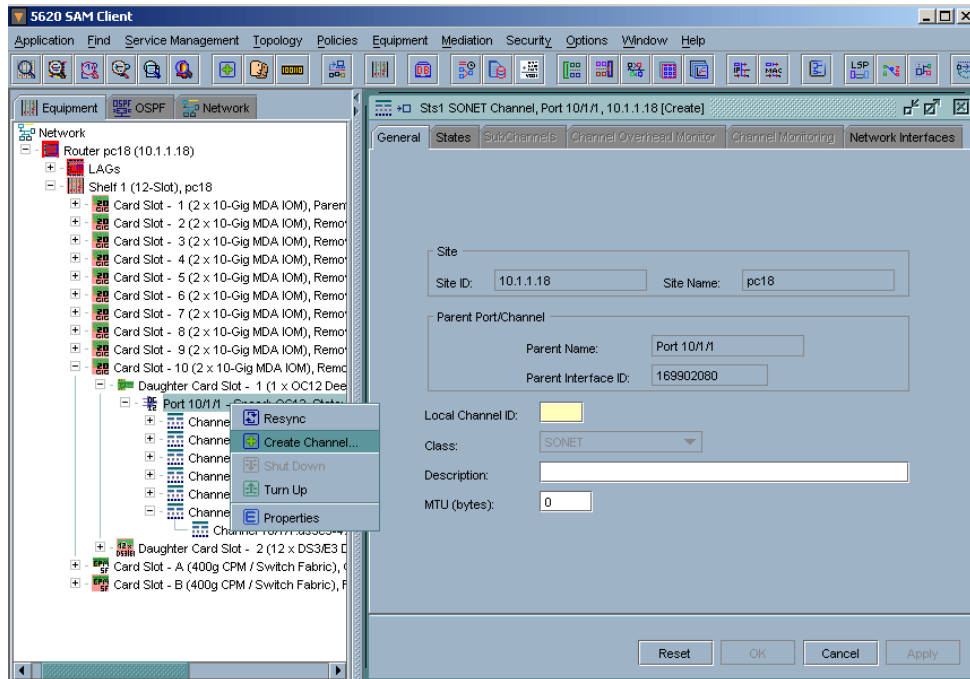
Procedure 14-9 To configure SONET clear channels and SONET STS1 sub-channels

Perform this procedure to configure SONET STS1 channels on ports that provide clear-channel or channelized services.

- 1 Right-click on the port and choose Create Channel.

The Create Channel form appears as shown in Figure 14-7 with the General tab button selected. If there are no channels available on that port, the Create Channel menu option menu is dimmed.

Figure 14-7 Create Channel configuration form - General



- 2 Configure the Local Channel ID field in the format: *STS3.STS1*.

For example, type 4.1 if the STS3 number is 4 and the STS1 number is 1. When you enter valid numbers, the color of the field changes from yellow to white.

If this is a clear-channel application, the Local Channel ID is configured automatically. Configure the other parameters as required.

- 3 Click on the Apply button to apply the changes on this form.

The STS1 channel appears in the navigation tree under the port of the daughter card. If this is a SONET STS1 sub-channel application continue to step 4.

- 4 Create the ds3 channel.
 - i Choose the STS1 channel that you created in the navigation tree and create the DS3 channel for a channelized 1xOC12 Deep Channel port.
 - ii Choose the Channelization Type as Channelized DS1 for a channelized 1xOC12 card. If you are configuring a SONET-based OCx card that is not channelized, you will not have the choice to make it channelized.
 - iii Click on the Apply button to apply the change.

- 5 Create the ds1 channel.
 - i Choose the ds3 channel that you created in the navigation tree and create a DS1 channel.
 - ii Configure the Local Channel ID. The range is 1 to 28 for DS1.
 - iii Click on the Apply button to apply the change.
 - 6 Create the ds0 channel group.
 - i Choose the ds1 channel that you created in the navigation tree and create a DS0 group.
 - ii Configure the Local Channel ID. The range is 1 to 24 for the DS0.
 - iii Configure the other parameters as required.
 - iv Click on the Apply button to apply the change.
 - 7 Click on the States tab button and change the administrative or operational states as required.
 - 8 Click on the Channel Group tab button to select timeslots as required.
 - 9 Click on the Terminations tab button to view information about the termination.
 - 10 Click on the Statistics tab button to view statistical information.
 - 11 Click on the Faults tab button to view information about faults that occur on the channel.
 - 12 After the channel object is created, you can open the Properties form and change the channel properties if required.
-

Procedure 14-10 To configure TDM channels

Perform this procedure to configure DS3 channel and children objects from a 12xDS3 port.

- 1 Right-click on the port that you want to configure and choose Create Channel from the contextual menu.

The Create Channel form appears. If there are no channels available on that port, the Create Channel menu option is dimmed.
- 2 Configure the ds3 channel.
 - a Choose the Channelization Type as Channelized DS1, if you want to channelize to the DS0 level.
 - b Choose None if this is a clear channel application.
 - i The Local Channel ID is configured automatically and the mode is always Access for TDM.

- ii** Configure the other parameters as required.
- 3** Click on the Apply button to apply the change.
If this is a Channelized DS1 application, continue to step 4.
- 4** Create the ds1 channel.
 - i** Choose the ds3 channel that you created in the navigation tree and create a DS1 channel.
 - ii** Configure the Local Channel ID. The range is 1 to 28 for DS1.
 - iii** Click on the Apply button to apply the change.
- 5** Create the ds0 channel group.
 - i** Choose the ds1 channel that you created in the navigation tree and create a DS0 group.
 - ii** Configure the Local Channel ID. The range is 1 to 24 for DS0.
 - iii** Click on the Apply button to apply the change.
- 6** Click on the States tab button and change the administrative or operational states as required.
- 7** Click on the Sub Channel tab button to select sub-channels to add or edit as required.
- 8** Configure the TDM port parameters to define how the channel operates. Once the channel object has been created you can open the Properties form and edit the channel properties as required.
 - i** Specify the administrative state as up from the States tab.
 - ii** Specify whether to use C-bit or m23 channel framing from the channel tab.
 - iii** Choose 16- or 32-bit cyclic redundancy checking (CRC precision).
 - iv** Specify the idle cycle flags as flags or ones.
 - v** Specify an internal (node timed) or lined (looped-timed) clocking source.
 - vi** Specify a loopback mechanism: Line, Internal, Remote, or None.
 - vii** Configure the FEAC Loop Respond parameter as false or true.
 - viii** Specify the Bit Error Insertion Rate.
 - ix** Specify the alarms to monitor.
 - x** Click on the OK button to accept the configuration.
 - xi** Configure the Message Data Link.

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 14-5 describes the MDL message options.

Table 14-5 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

- 9** Click on the Statistics tab button to view statistical information.
 - 10** Click on the Faults tab button to view information about faults that occur on the channel.
-

15 — Equipment management using the equipment manager

- 15.1 Equipment manager overview 15-2**
- 15.2 Workflow to manage equipment using the Equipment manager 15-7**
- 15.3 Equipment manager menu 15-8**
- 15.4 Equipment manager procedures list 15-8**
- 15.5 Equipment manager procedures 15-8**

15.1 Equipment manager overview

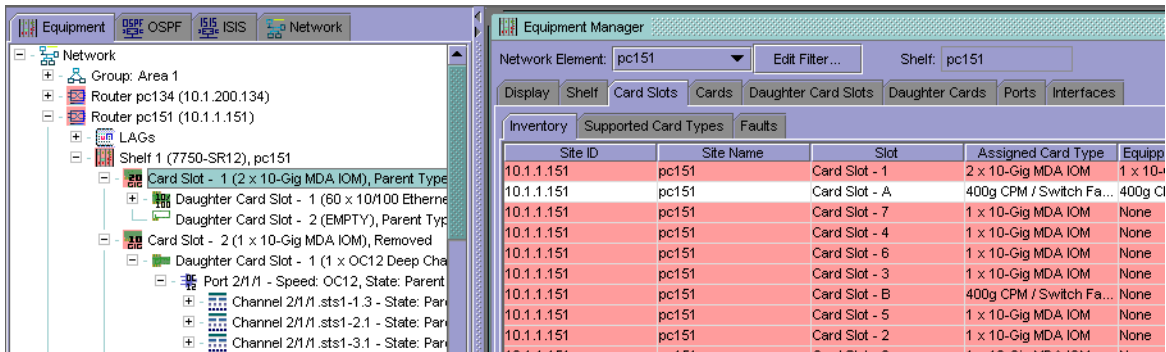
The 5620 SAM equipment manager allows network administrators and operators to do the following:

- filter different views and information for the managed devices using the Network Element Filter
- view and use a graphical representation of the shelf to configure equipment objects and get statistical information about the nodes in their administrative domain
- view the services that traverse or terminate on equipment
- provision and pre-provision equipment to prepare the equipment for the creation of subscriber services
- view, configure, monitor the state of, and manage the following physical elements of the hardware:
 - a managed device
 - each device has one shelf, which is the physical shelf
 - up to 12 card slots where cards are inserted into the device
 - card slots contain cards
 - cards contain up to two daughter card slots, also known as I/O modules
 - each daughter card slot contains a daughter card
 - daughter cards contain ports
 - ports contain channels
 - up to 64 LAGs per managed router, a logical object which joins multiple Ethernet ports into a single port to aggregate bandwidth
 - internal and external storage devices (flash memory)
- configure network and access policies for network objects, such as ingress buffer policies for a port
- manage hardware fault conditions

Equipment manager forms

The equipment manager provides a tab for each equipment component. Figure 15-1 shows an example of the equipment manager form displayed with the Card Slots tab selected. The parameters displayed on each form are specific to the service that you are configuring. There are configurable and read-only parameters displayed from each tab. The read-only parameters are inherited from other configurations through device discovery.

Figure 15-1 Equipment manager form - Card Slots



Display tab

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.

Shelf tab

The Shelf tab displays general information about the managed physical equipment.

The 7750 SR configurations that are managed include the following shelf types:

- 1-slot with 1 I/O slot that supports 2 cards
- 4-slots with 3 I/O slots that support 6 cards. The slots are numbered from top to bottom.
- 7-slots with 5 I/O slots that support 10 cards. The slots are numbered from top to bottom
- 12-slots with 10 I/O slots that support 20 cards. The slots are numbered from left to right.

The 7450 ESS configurations that are managed include the following shelf types:

- 1-slot with 1 I/O slot that supports 2 cards
- 7-slots with 6 I/O slots that support 12 cards. The slots are numbered from top to bottom.

Click on the Properties option from the contextual menu in the Equipment tab navigation tree to display several tabs that show shelf information and chassis environment data, including the temperature, fans, power supplies, LEDs, storage, and fault information.

- The Fan Trays tab displays details about each fan tray. Double-click on a row in the fan tray list to view additional information, such as operational state and speed.
- The Power Supply Trays tab displays details about the router power supply, including voltage and temperature.
- The LED Panel tab displays the status of LEDs on the device, including the number of critical, major, and minor LEDs currently showing on the device.
- The Card Slots tab displays all the cards in all the slots.
- The Hardware Environment tab displays the current and threshold temperature settings of the configured cards.
- The Statistics tab displays CPU and memory statistics.
- The Faults tab lists all alarms raised against objects in the shelf.

Card Slots tab

The Card Slots tab displays the cards that are installed on or provisioned for the node, the supported card type for each slot, and fault information. To pre-provision a slot, the allowed card types, and the line card must be specified.

- The Inventory tab displays cards configured in the slots.
- The Supported Card Types tab indicates the types of cards that can be configured for the slots.
- The Faults tab lists alarms raised against card slots.

Cards tab

The Cards tab has several tabs to display the line or system daughter cards, also called IOM cards, that are installed on, pre-provisioned, or provisioned for the node.

- The Inventory tab displays the card type, serial number, revision number, and equipment state.
- The Processors tab displays information about the two processors Control cards, also called the CPM or switch fabric cards. Double-click on the A or B slot Control card for information about the control processors and switch fabric processors.
- The Software tab displays the card version, boot code information, and state.
- The Environment tab displays card environment information, for example, temperature thresholds.
- The Faults tab displays alarm information for card and card child objects, such as ports.

Daughter Card Slots tab

The Daughter Card Slots tab displays the daughter cards that are provisioned for the node, the supported daughter card types, and fault information. To pre-provision a daughter card slot, the slot, and daughter card types must be specified before the daughter card is configured.

Choose a specific daughter card type for the slot. The daughter card can be pre-provisioned but a daughter card must be provisioned before ports can be configured. Ports can be configured when the daughter card is properly provisioned.

Up to two daughter cards can be provisioned on an IOM. Only one daughter card can be provisioned per IOM daughter card slot. To modify a daughter card slot, shut down all port associations.

The additional daughter card slots tabs include:

- The Inventory tab lists the daughter card slots and the daughter cards configured for the slots.
- The Supported Daughter Card Types tab lists the types of cards allowed and supported in each daughter card slot.
- The Faults tab displays alarm information for daughter card slots and daughter card slot children objects, such as ports.

Daughter Cards tab

The Daughter Cards tab displays daughter card information, including the daughter card slot ID, daughter card types, serial numbers, manufacture date, hardware revision, administrative and operational states, maximum number of ports, network ingress buffer policy ID, and fault information.

The additional daughter card tabs include:

- The Inventory tab lists the daughter cards configured for the slots.
- The Faults tab displays alarm information for daughter cards and daughter card children objects, such as ports.

Ports tab

The Ports tab displays information about physical ports, SONET or SDH channels, TDM channels, link aggregation groups, protocols, terminations, and faults.

Figure 15-2 shows an example of a port configuration form with the General tab selected.

Figure 15-2 Example of a port configuration form - General

Physical Port - Port 1/1/16, 10.1.200.51 [Edit]

General States Ethernet Terminations L2 Interfaces L3 Interfaces Qos Pool Statistics Faults

Site

Site ID: 10.1.200.51 Site Name: sim200.51

Name: Port 1/1/16 CLI Name: 1/1/16

Interface ID: 19398656

Class: Fast Ethernet

Description: 10/100 Ethernet TX

Hardware MAC: 90-33-01-01-00-10

Configured MAC: 90-33-01-01-00-10

Mode: Access

Encap Type: Null

Speed: 100

Actual Speed (KBytes): 0

MTU (bytes): 1514

Hold Time

Hold Time Up: 0 Hold Time Down: 0

For each network and access port, you can view and configure parameters using the tab buttons.

- The General tab includes port mode, MTU sizes, configured MAC addresses, and encapsulation type parameters at the connection termination point.
- The Ethernet tab includes frame size parameters.
- The Policies tab includes ingress and egress buffer policies.
- The Terminations tab lists services or interfaces that terminate on the port.
- The Interface tab for network ports lists IP routing information and configuration parameters.
- The Services tab lists subscriber services that use the Layer 2 or Layer 3 interface associated with the port.
- The Statistics tab lists the statistics that are collected for the port.

Additional ports tabs include:

- The Physical Ports tab lists all physical ports on the device.
- The SONET Channels tab lists all SONET channels configured on the device.
- The Link Aggregation Groups tab lists all configured LAGs on the router.
- The Protocols tab lists all protocols that can be configured or are enabled on each port.
- The Terminations tab lists the number of connections on each endpoint, the encapsulation type of the endpoint, and bandwidth usage information.
- The TDM Channels tab lists all TDM channels configured on the device.
- The Statistics tab lists interface, SONET or SDH, TDM, and LAG statistics for the ports.
- The Faults tab lists alarms raised against the device.

Interfaces tab

The Interfaces tab displays the interfaces that are configured for the port, including the device interfaces and the IP addresses. You can select the interface and click Edit to reconfigure the interface. See the *7750 SR OS Router Guide* for more information about IP network routing configuration.

The interfaces tabs include:

- The Network Interfaces tab lists the ports configured for network access.
- The L2 Interfaces tab, on the Ethernet and SONET forms, lists the ports and channels configured as Layer 2 interfaces, and the services using those Layer 2 interfaces.
- The L3 Interfaces tab, on the Ethernet and SONET forms, lists the ports and channels configured as Layer 3 interfaces, and the services using those Layer 3 interfaces.
- The Address tab lists routing instance information.
- The Faults tab lists routing alarms raised against the interfaces.

15.2 Workflow to manage equipment using the Equipment manager

- 1 Ensure the routers are configured before they are discovered by the 5620 SAM.
- 2 Access the equipment and begin configuration and management.
 - i Choose Equipment→Equipment Manager from the 5620 SAM main menu.
 - ii Use the equipment manager to edit or view objects and configuration parameters.
 - iii Edit the properties of objects as required in equipment manager.

15.3 Equipment manager menu

Table 15-1 lists the menu item to use the equipment manager.

Table 15-1 5620 SAM equipment manager menu

Menu option	Task
Equipment→Equipment Manager	Open the equipment manager form to view and edit existing objects.

15.4 Equipment manager procedures list

Table 15-2 lists the procedures to configure equipment using the equipment manager.

Table 15-2 5620 SAM equipment manager procedures list

Procedure	Purpose
To use the network element filter	To narrow the range of devices that you can view using the equipment manager.
To change the configuration of devices using the equipment manager	To configure an object using the equipment manager.

15.5 Equipment manager procedures

Use the following procedures to manage equipment using the equipment manager.

Procedure 15-1 To use the network element filter

The network element filter, which opens when the equipment manager is opened, filters specific information to the equipment manager forms for a specific network device. You can use the network element filter to quickly see a snapshot of various selected parameters or click on the OK button of the Simple filter to view or edit all the forms and configured parameters in the equipment manager for the managed device.

- 1 Choose Equipment→Equipment Manager from the 5620 SAM main menu.
The network element filter opens on top of the equipment manager form.
- 2 You can close the filter form or create a filter.
 - a Click on the OK button to close the filter form and access the equipment manager form.

The network element filter form closes and the equipment manager form is brought to the foreground.

- b** Click on the Simple radio button to perform a simple search of parameters for a snapshot of the state of the specified parameter.
 - i** Choose a parameter in the Unused Properties box.
 - ii** Click on the right-facing arrow.

The parameter moves to the Filtered Properties box.
 - iii** Click on the OK button.

The network element filter form closes and the equipment manager form is brought to the foreground.
 - 3** Choose a device from the Network Element parameter to select a device or toggle between the various managed network elements in the navigation tree.
-

Procedure 15-2 To change the configuration of devices using the equipment manager

An object must be created before it can be configured. A created object is seen in the navigation tree. See chapter 14 for more information about using the navigation tree.

- 1** Right-click on a discovered device in the navigation tree and choose Equipment Manager from the contextual menu.

The Equipment Manager Filter and Network Element Filter forms are displayed.
 - 2** Select the filter type and filtered properties, as described in Procedure 15-1.
 - 3** Click on the OK button.

The 5620 SAM displays a graphical representation of the shelf under the Display tab.
 - 4** Choose tabs to configure the equipment parameters in the sequence displayed.
 - a** Double-click on any of the slots displayed under the Display tab to open the Properties form for the slot and create or edit the parameters of an object in the shelf.
 - b** Select a parameter in any of the list forms and click on the Edit button to access the parameters that can be configured.
 - c** Double-click on any object in any form to show the object Properties form.
 - 5** Save the configuration changes, as required.
-

16 — Router configuration

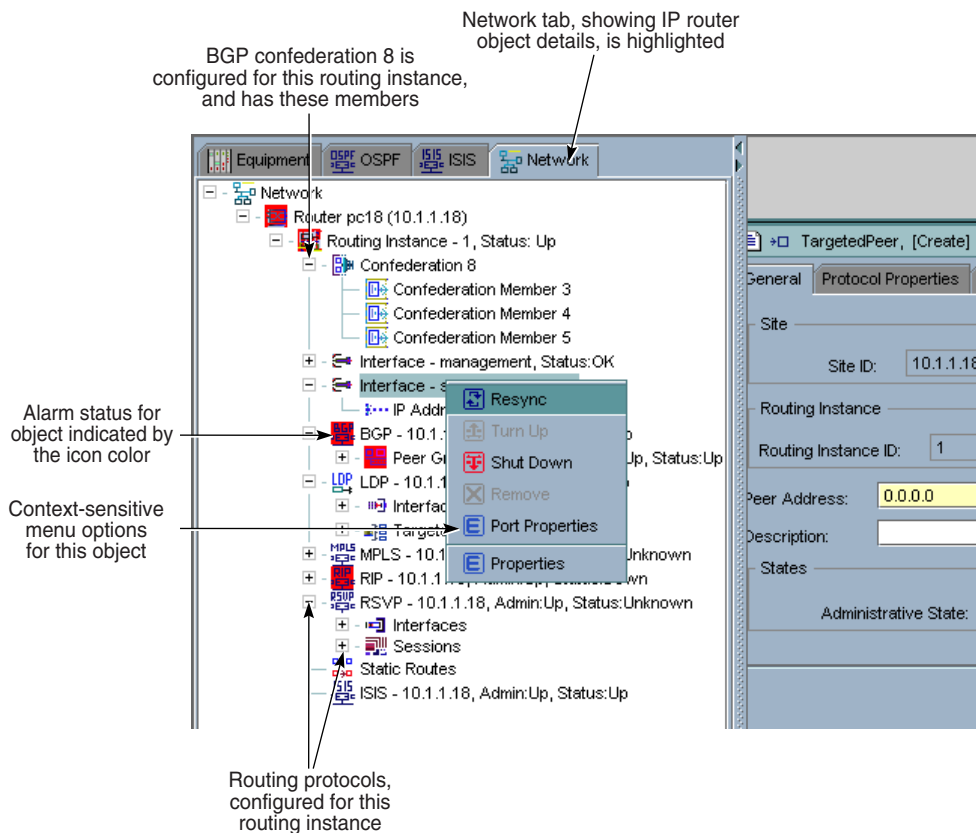
- 16.1 Router configuration overview 16-2**
- 16.2 Workflow to configure routers 16-3**
- 16.3 Router configuration menus 16-4**
- 16.4 Router configuration procedures list 16-5**
- 16.5 Router configuration procedures 16-5**

16.1 Router configuration overview

The 5620 SAM allows you to view router parameters and configure network interface parameters. You can use the Network tab on the 5620 SAM GUI navigation tree to view and configure parameters that set and manage the IP routing functionality of the 7750 SR.

Figure 16-1 shows the IP router objects in the Network tab of the navigation tree.

Figure 16-1 Router objects



17336

Layer 3 interfaces, sometimes referred to as network interfaces, are logical IP objects defined on physical port, such as an Ethernet port. A Layer 3 interface:

- has an IP address and subnet mask
- is configured with QoS policy settings
- associates its IP address with a physical port or channel
- has its physical port or channel cabled to another router
- has enabled routing protocols

The physical connection of one router to another router is through its port or channel. However, the Layer 3 interface determines its IP connectivity. The Layer 3 interface passes both routing information using a routing protocol, such as OSPF, and passes IP traffic.

The system interface is associated with a network entity, such as a specific router, 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 router 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 with a 32-bit subnet mask. The system interface is used as the router identifier by higher-level protocols such as OSPF and BGP. See chapter 17 for more information about routing protocols.

When configuring routers, you configure the routing protocols used and the topology of how packets are handled between different routers 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, known 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 routers, which are not area border routers, and belonging to the same area, have identical topological databases.

Routers that are aware of more than one area are called area border routers. In this case, all routers 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 router. BGP uses the information and path parameters to compile a network topology.

See the *7750 SR OS Router Guide* for more information about the parameters that you can configure.

16.2 Workflow to configure routers

- 1 Use the CLI to configure these router parameters:
 - system name
 - router ID

See the *7750 SR OS Router Guide* for more information about the parameters to configure.

- 2 Configure L3 interfaces. The L3 interfaces will be associated with network ports. There are network and system interfaces.
 - assign names
 - associate IP addresses
 - specify the interface as a network or system interface
 - associate a network port with the Layer 3 interface
 - configure appropriate routing protocolsEnable BGP, MPLS, RIP, LDP, OSPF, IS-IS, and RSVP on the interfaces as required.
See chapter 17 for more information about routing protocol configuration and parameters.
- 3 Cable the network ports on the router to the network ports on other routers.
- 4 Configure these key router parameters using the 5620 SAM:
 - Enable BGP, MPLS, RIP, LDP, OSPF, IS-IS, and RSVP routing protocols on the router, 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.
 - router-wide AS settings
- 5 Use the 5620 SAM to create static routes as required.
- 6 Use the 5620 SAM to configure a routing policy.

Configure an AS and confederations for BGP (optional).

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 17 for more information about BGP configuration.
- 7 Use the 5620 SAM to create MPLS administrative groups and assign the groups to MPLS interfaces, LSPs, and LSPs paths as required.

16.3 Router configuration menus

To configure managed equipment as routers, select the Network tab on the navigation tree.

16.4 Router configuration procedures list

Table 16-1 lists the procedures necessary for router configuration.

Table 16-1 5620 SAM router configuration procedures list

Procedure	Purpose
To configure router routing instance parameters	To configure the router routing instance parameters
To configure or modify a Layer 3 interface	To configure the following interfaces: <ul style="list-style-type: none"> • network interface • system interface • interface ICMP • management interface
To configure an AS and confederations (optional)	See the BGP information contained in chapter 17.
To configure a routing policy	To control the size and content of the routing tables, the routes that are advertised, and the best route to a destination
To configure an MPLS administrative group policy	To configure MPLS administrative groups that can be assigned to MPLS interfaces, LSPs, and LSP paths.
To configure a static route	To create static route entries for the network and access routes

16.5 Router configuration procedures

The following procedures describe how to configure routers.

Procedure 16-1 To configure router routing instance parameters

Perform Procedure 16-1 to configure router parameters. See the *7750 SR OS Router Guide* for more detailed parameter information.

- 1 Select the Network tab on the navigation tree.
- 2 Navigate to a routing instance.
The navigation path is Network→Router→Routing Instance.
- 3 Right-click on the routing instance icon and choose Properties from the contextual menu.

The 5620 SAM displays the Routing Instance form. Figure 16-2 shows the Routing Instance form with the Protocols tab button selected.

Figure 16-2 Routing Instance form - Protocols

- 4 Configure the routing instance parameters. Table 16-2 describes the tabs to configure the minimum requirements for a router.

Table 16-2 Routing instance configuration form

Tab	Description
General	To set the Administrative State parameter to Up
Protocols	To enable supported protocols including BGP, MPLS, RIP, LDP, OSPF, IS-IS, and RSVP. Choose the check box next to the routing protocol to enable the protocol. The supported protocols are displayed in the navigation tree as subitems in the routing instance. Click on the Edit button to configure the routing protocols. See chapter 17 for more information about routing protocol configuration using the GUI.
Routing	To specify AS and confederation parameters (optional), and to enable the re-evaluation of route policies. See chapter 17 for more information about AS and confederation parameters for BGP using the GUI
Interfaces	To specify and add Layer 3 interfaces. See Procedure 16-2 for more information about creating additional Layer 3 interfaces.

(1 of 2)

Tab	Description
Address	To configure IP addressing information for the Layer 3 interfaces. Choose an address in the list and click on the Edit button. The IP address information configuration form appears. You can configure the following from the IP address information configuration form. <ul style="list-style-type: none"> IGP inhibit to specify whether the secondary IP address for the Layer 3 interface should not be recognized as a local interface by the running IGP the broadcast address format faults associated with the IP address on the Layer 3 interface
Static Routes	To view a list of static routes and to add static routes. See Procedure 16-5 for more information.
BGP Confederations	To view and create BGP confederation configurations. See chapter 17 for more information about BGP confederation configuration using the GUI.
Statistics	To view route statistics for this routing instance.
Service Address Ranges	To provide a mechanism to reserve one or more IP address ranges for use by services, such as IES.
Faults	Alarms raised against the routing instance, or related alarms that affect the routing instance.

(2 of 2)

- 5 Click on the Apply button to save the changes.
- 6 Verify the action.
- 7 Close the form.

Procedure 16-2 To configure or modify a Layer 3 interface

Perform Procedure 16-2 to configure Layer 3 interface parameters. The interfaces you configure or modify include:

- Layer 3 interface
- ICMP interface
- system interface
- management interface

See the *7750 SR OS Router Guide* for more information about using CLI to configure interfaces.

- 1 Select the Network tab on the navigation tree.
- 2 Navigate to a routing instance.
The navigation path is Network→Router→Routing Instance.
- 3 Create a new Layer 3 interface, or modify an existing Layer 3 interface:
 - a Right-click on the routing instance icon and choose Create Interface from the contextual menu to create a new Layer 3 interface.

The 5620 SAM displays the Create Network Interface routing instance series of configuration forms, as shown in Figure 16-3. Continue to step 4.

Figure 16-3 Routing instance configuration form - Define General Properties step

The screenshot shows a web-based configuration interface for a routing instance. The title bar reads "Create Network Interface - Routing Instance - 1, 10.1.1.18". On the left, a "Steps" sidebar lists eight steps, with "1. Define General Properties" highlighted in cyan. The main area is titled "Define General Properties" and contains the following fields:

- Interface ID: Auto-Assign ID
- Name:
- Description:
- Administrative State:
- MAC Address:
- Allow Directed Broadcasts:
- Class:

At the bottom of the form are four buttons: "< Back", "Next >", "Finish", and "Cancel".

- b** Choose a Layer 3 interface, right-click and choose Properties to modify the existing Layer 3 interface.

The 5620 SAM displays the Network Interface configuration form.

Modify the existing Layer 3 interface parameters. Figure 16-4 shows the Network Interface configuration form with the Port tab selected.

Figure 16-4 Network Layer 3 interface configuration form - Port

Network Interface - 2, Routing Instance - 1, 10.1.1.23 [Edit]

General Port Policies Protocols Address ICMP ARP NTP Faults

Port: N/A

Port ID: 0

Encap Type: unspecified

Encap Value: 0

Provisioned Max Frame Size: 1500

Actual Max Frame Size: 0

Max Frame Size Mismatch:

Underlying Port State: No Association

Table 16-3 describes the tabs to choose, as shown when you modify an existing routing interface. Continue to step 14.

Table 16-3 Network Interface configuration form

Tab	Description
General	To assign a MAC address to the interface, the administrative state as up or down, whether to allow direct broadcasts, and the numbered or unnumbered class.
Port	To create an association between the Layer 3 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.

(1 of 2)

Tab	Description
Protocols	To view a list of protocols that are enabled on the interface, and to add protocols. The protocols are: <ul style="list-style-type: none"> • MPLS • OSPF • LDP • RSVP • ISIS • RIP <p>You then associate the Layer 3 interface with a protocol.</p>
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.
ICMP	To configure ICMP parameters related to mask replies and redirects, unreachable, and TTL properties.
ARP	To configure the minimum time in seconds that an ARP entry is stored in the ARP table. Click on the Add button to set static ARP IP and MAC address parameters.
NTP	To enable SNTP broadcasts on the network interface
Statistics	To view Layer 3 network interface statistics
Faults	Alarms raised against the network interface, or related alarms that affect the network interface.

(2 of 2)

- 4 Provide a name and description for the new Layer 3 interface.
- 5 Set the administrative state to up or down.
- 6 Configure the MAC address.
- 7 Enable or disable direct broadcasts.
- 8 Specify the class parameter. A numbered interface means the Layer 3 interface has its own IP address. Unnumbered means the router ID is advertised.
- 9 Click on the Next button.
- 10 Specify the IP address information for the Layer 3 interface.
 - i Click on the Add button.
The IP address routing instance form appears.
 - ii Configure the IP address for the numbered interface. Set the subnet mask and broadcast address format.

You can specify one primary and many secondary IP address for the Layer 3 interface.
 - iii Specify the Broadcast Address Format parameter.
 - iv Enable or disable IGP inhibit.
 - v Click on the OK button to save the changes.

- 11 Click on the Next button.
 - 12 Associate the Layer 3 interface with a physical port.
 - i Click on the Select button.

The Select Port form appears.
 - ii Choose a port from the list.
 - iii Click on the OK button.

The port is associated with the Layer 3 interface.
 - 13 Specify the remaining QoS, filter, ARP, ICMP, and NTP parameters as appropriate. Use the Next button to proceed through each step.
 - network policies are used to determine QoS settings based on the packet DSCP bits on the ingress and egress of the network
 - ACL filters are used to filter out IP traffic that matches user-defined criteria
 - ICMP settings specify how ping commands work
 - ARP settings are used to statically associate IP or MAC addresses
 - enabling NTP means the Layer 3 interface sends NTP broadcasts to neighboring routers
 - 14 Click on the Finish button if you are creating a new network interface, or click on the Apply button to save changes to an existing network interface.
 - 15 Cable the network ports or channels of the router, with Layer 3 interfaces enabled, to other routers configured the same way.
 - 16 Configure routing protocols, as described in chapter 17.
-

Procedure 16-3 To configure a routing policy

Perform Procedure 16-3 to configure routing policies. See the *7750 SR OS Router Guide* for more detailed parameter information. There are no default routing policies.

The 5620 SAM supports routing policy configuration on the 7750 SR, which supports two databases for routing information. The routing database contains the routing information learned by the routing protocols. The forwarding database is composed of the routes actually used to forward traffic through a router. In addition, link state databases are maintained by IGP's such as ISIS and OSPF.

Routing protocols calculate the best route to each destination and place these routes in a forwarding table. The routes in the forwarding table are used to forward routing protocol traffic, sending advertisements to neighbors and peers.

For example, you can configure a routing policy that will not place routes associated with a specific origin in the routing table. Those routes will not be used to forward data packets to the intended destinations and the routes are not advertised by the routing protocol to neighbors and peers. 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.

- 1 Select the Network tab on the navigation tree.
- 2 Navigate to a routing instance.
The navigation path is Network→Router→Routing Instance.
- 3 Right-click on the routing instance icon and choose Properties from the contextual menu.
The 5620 SAM displays the Routing Instance form.
- 4 From the General Tab, click on the Edit Routing Policies button.
The 5620 SAM displays the Routing Policy Manager form with the General tab button selected, as shown in Figure 16-5.

Figure 16-5 Routing Policy Manager form - General

The screenshot shows a window titled "Routing Policy Manager - [pc18] [Edit]". The window has several tabs: "General", "AS Paths", "Communities", "Dampings", "Policy Statements", "Prefix Lists", and "Faults". The "General" tab is selected. The form contains the following fields:

- Site** (label)
- Site ID:** 10.1.1.18
- Site Name:** pc18
- Triggered Re-evaluation of Route Policies:** false (dropdown menu)

At the bottom of the form, there are five buttons: "Resync", "Reset", "OK", "Cancel", and "Apply".

5 Configure the routing policy parameters in the following sequence, using the tabs on the Routing Policy Manager form:

- General
- AS paths
- Communities
- Dampings
- Policy Statements
- Prefix Lists
- Faults

Table 16-4 describes the tabs that you can choose to configure the parameters. See the “Route Policies” chapter in the *7750 SR OS Router Guide* for specific information about the parameters.

Table 16-4 Routing Policy Manager form

Tab	Description
General	Displays the site name and site ID and allows you to configure the Triggered Re-evaluation of Route Policies parameter. The options are true or false.
AS Paths	<p>Click on the Add button to create new AS paths, or click on the Edit button to modify existing AS paths.</p> <p>In the AS path form that opens, you can configure the following parameters.</p> <ul style="list-style-type: none"> • Path Name. The range is 1 to 32 characters • Description. The range is 0 to 80 characters. • Regular Expression. The range is 1 to 80 characters.
Communities	<p>Click on the Add button to create new communities, or click on the Edit button to modify existing communities.</p> <p>In the Community form that appears, you can add community members and configure the Community Name parameter. The range is 1 to 32 characters.</p>
Dampings	<p>Click on the Add button to create new dampings, or click on the Edit button to modify existing dampings.</p> <p>In the Dampings form that appears, you can configure the following parameters.</p> <ul style="list-style-type: none"> • Damping Name. The range is 1 to characters. • Half Life. The range is 0 to 45. • Reuse. The range is 0 to 20 000. • Suppress. The range is 0 to 20 000. • Max. Suppression. The range is 0 to 720.

(1 of 2)

Tab	Description
Policy Statements	<p>Click on the Add button to create policy statements, or click on the Edit button to modify existing policy statements. In the Create Routing Policy form that appears, follow the steps to configure the following parameters.</p> <ul style="list-style-type: none"> • Policy Statement Name. The range is 1 to 32 characters. • Description. The range is 0 to 80 characters. • Default Action. The options are Reject or Accept. <p>Click on the Next button.</p> <p>From the Configure policy entries, click on the Add button to create policy entries, or click on the Edit button to modify existing policy entries.</p> <p>The Create Routing Policy Entry form appears. Follow the steps to configure the following parameters. Click on the Next button to proceed to the next step. You can configure multiple policy entries.</p> <ul style="list-style-type: none"> • Entry ID. The range is 1 to 65 535. • Description. The range is 0 to 80 characters. • Action. The options are None, Reject, or Accept. • From Criteria: <ul style="list-style-type: none"> • AS Path Name. The range is 0 to 32 characters. • Protocol. The options are None, Direct, Static, BGP, ISIS, OSPF, RIP, Aggregate, BGP-VPN, IGMP, or PIM • Origin. The options are None, IGP, EGP, or Incomplete • Community List Name. The range is 0 to 32 characters. • Interface Name. The range is 0 to 32 characters. • ISIS Route Level. The options are 0, 1, or 2. • ISIS External Route. The options are true or false. • OSPF Route Type. The options are 0, 1, or 2. • OSPF Area. Enter an IP address in the format xxx.xxx.xxx.xxx • OSPF Origin. The options are None, IGP, EGP, or Incomplete. • OSPF Area Set. The options are true or false. • Neighbor IP Address. Enter an IP address in the format xxx.xxx.xxx.xxx • Neighbor Prefix List Name. The range is 0 to 32 characters. • Prefix Lists. Enter up to five prefix list. The range is 0 to 32 characters. • To Criteria: <ul style="list-style-type: none"> • Protocol. The options are None, BGP, ISIS, OSPF, RIP, BGP-VPN. • ISIS Route Level. The options are 0, 1, or 2. • Neighbor IP Address. Enter an IP address in the format xxx.xxx.xxx.xxx • Neighbor Prefix List Name. The range is 0 to 32 characters.
Prefix Lists	<p>Click on the Add button to create new prefix lists, or click on the Edit button to modify existing prefix lists. Configure the Prefix List Name parameter. The range is 1 to 32 characters.</p> <p>Click on the Prefix List Members tab button.</p> <p>Click on the Add to create prefix list members, or click on the Edit button to modify existing prefix list members. In the Prefix List Member form that appears, configure the parameters. You can configure multiple prefix list members.</p> <ul style="list-style-type: none"> • Prefix. Enter an IP address in the format xxx.xxx.xxx.xxx • Mask. Enter a network mask in bitmask format. The range is 0 to 32. • Type. The options are Exact, Longer, Through, Range. • Depending on the option that you select for the Type parameter, you can configure the Begin Length and Through Length parameters. The range for both parameters is 24 to 32. The value is in bitmask format.
Faults	Displays and view alarms related to routing policy management.

(2 of 2)

Procedure 16-4 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, routers will 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 router 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.

See the *7750 SR OS Services Guide* for more information about MPLS administrative groups and CSPF.

This procedure describes how to create MPLS administrative groups. Table 16-5 describes where to find information about assigning MPLS administrative groups to MPLS interfaces, LSPs, and LSP paths.

Table 16-5 MPLS administrative group assignments

To assign groups to	See procedure
MPLS interfaces	"To create MPLS interfaces" in chapter 18
LSPs	"To create LSPs" in chapter 18
LSP paths	"To configure LSP paths" in chapter 18

- 1 Choose Policies→Admin Group (MPLS) Policy Manager from the 5620 SAM main menu.

The Admin Group (MPLS) Policy Manager form opens.

- 2 Click on the Create Admin Group Policy button.

The MPLS administrative group policy form appears with the General tab button selected, as shown in Figure 16-6.

Figure 16-6 MPLS administrative group form — General

The screenshot shows a configuration window titled "Admin Group (MPLS), Global Policy- [Create]". It features a tabbed interface with "General", "Definitions", "LSPs", "LSP Paths", and "Interfaces" tabs. The "General" tab is selected. In the main area, there is a "Displayed Name" label followed by a yellow text input field, and a "Value:" label followed by a spin box containing the number "0". At the bottom of the window, there are four buttons: "Reset", "OK", "Cancel", and "Apply".

Configure the parameters.

- i Enter a name for the administrative group.
- ii Enter a value for the administrative group. The value is in 32 bit mask format.

The value is used by MPLS interfaces to advertise administrative group associations using CSPF. The value must be identical across all routers within a single domain. The range is 0 to 31.

- 3 Click on the Apply button to save the policy.

The MPLS administrative group policy form is refreshed and the tabs are selectable. Table 16-6 describes the tabs that you can choose to configure the parameters.

Table 16-6 MPLS administrative group form

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 Paths	Lists and allows you to manage LSP paths to which the administrative group has been assigned.

(1 of 2)

Tab	Description
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.

(2 of 2)

- Click on the Distribute button to manually distribute the administrative group policy locally to routers. Policies are also automatically distributed to routers when they are used by resources on the router.

Procedure 16-5 To configure a static route

- Select the Network tab on the navigation tree.
- Navigate to the static routes icon.
The navigation path is Network→Router→Routing Instance→Static Routes.
- Right-click on the static routes icon and choose Create Static Route from the contextual menu.

The 5620 SAM displays the Static Route (Create) form, as shown in Figure 16-7.

Figure 16-7 Static Route (Create) form

Static Route ID: Auto-Assign ID

Routing Instance ID: Routing Instance Name:

Destination

Destination: Mask:

Type: IP Address:

Unnumbered Interface:

Other

Preference:

Metric:

Administrative State: Operational State:

- 4 Configure the parameters.
 - auto-assign an ID or choose an ID for the static route
 - set the Destination parameter to identify the IP address and the Mask parameter to identify the IP address subnet mask, if applicable
 - set the Type parameter to indicate the type of static route, which can be Next Hop, Indirect, or Black Hole
 - choose an Unnumbered Interface by clicking on the Select button, and choosing an interface from the list, if applicable
 - specify the Preference and Metric parameters, if applicable
 - set the Administrative State parameter to Up or Down to turn up or shut down the static route
 - 5 Click on the OK button.
-

17 — Routing protocol configuration

- 17.1 Routing protocol configuration overview 17-2**
- 17.2 Workflow to configure routing protocols 17-10**
- 17.3 Routing protocol configuration menus 17-11**
- 17.4 Routing protocol configuration procedures list 17-11**
- 17.5 Routing protocol configuration procedures 17-12**

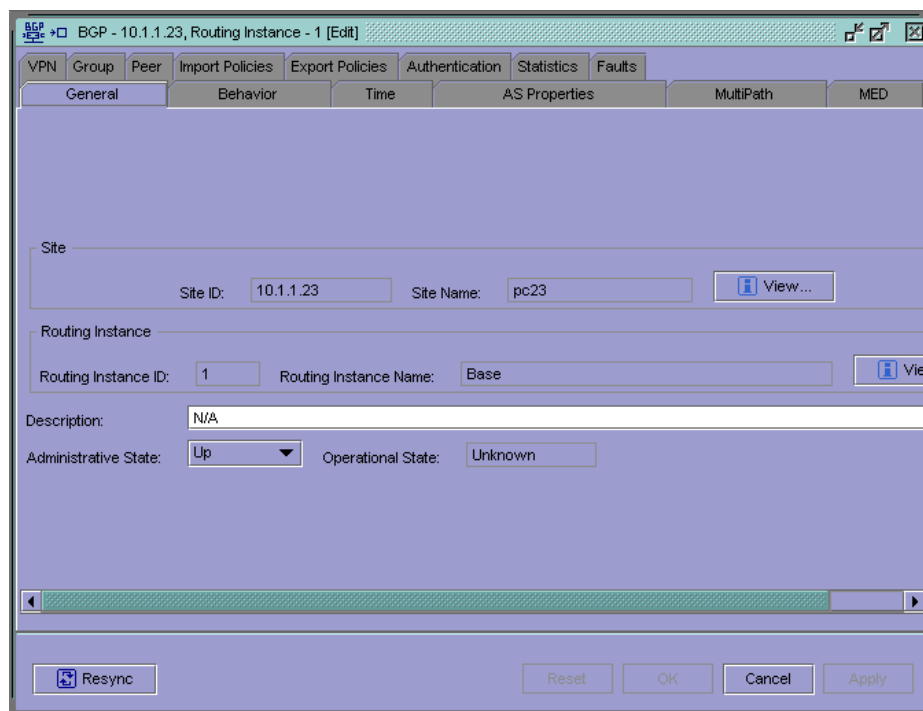
17.1 Routing protocol configuration overview

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, ISIS, and OSPF tabs on the 5620 SAM GUI navigation tree to view and configure parameters that set and manage the routing protocol support of the 7750 SR. The routing protocols are enabled on the devices when you configure the devices. The Layer 3 interfaces are configured when you configure the routing instance on the device. You can then configure the routing protocols for the specific Layer 3 interfaces.

Configuration is done using configuration forms, as shown in example Figure 17-1.

Figure 17-1 Example BGP configuration form - General



The screenshot displays the 'BGP - 10.1.1.23, Routing Instance - 1 [Edit]' configuration window. The 'General' tab is selected, showing fields for Site ID (10.1.1.23), Site Name (pc23), Routing Instance ID (1), and Routing Instance Name (Base). The Administrative State is set to 'Up' and the Operational State is 'Unknown'. A 'Resync' button is visible at the bottom left, and 'Reset', 'OK', 'Cancel', and 'Apply' buttons are at the bottom right.

Supported routing protocols include:

- BGP
- RIP
- OSPF
- RSVP
- LDP
- ISIS

See the *7750 SR OS Router Guide* for more information about these routing protocols.

BGP

There are two types of BGP.

- BGP
- MP-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.

- Within an AS, IBGP is used to communicate with peers within an autonomous system. Routes received from a 7750 SR in the same autonomous system are not advertised to other devices in the same autonomous system but can be advertised to an EBGP peer.
- Outside of an AS or between ASs, EBGP is used to communicate with peers in different autonomous systems. Routes received from a device in a different AS can be advertised to both EBGP and IBGP peers.

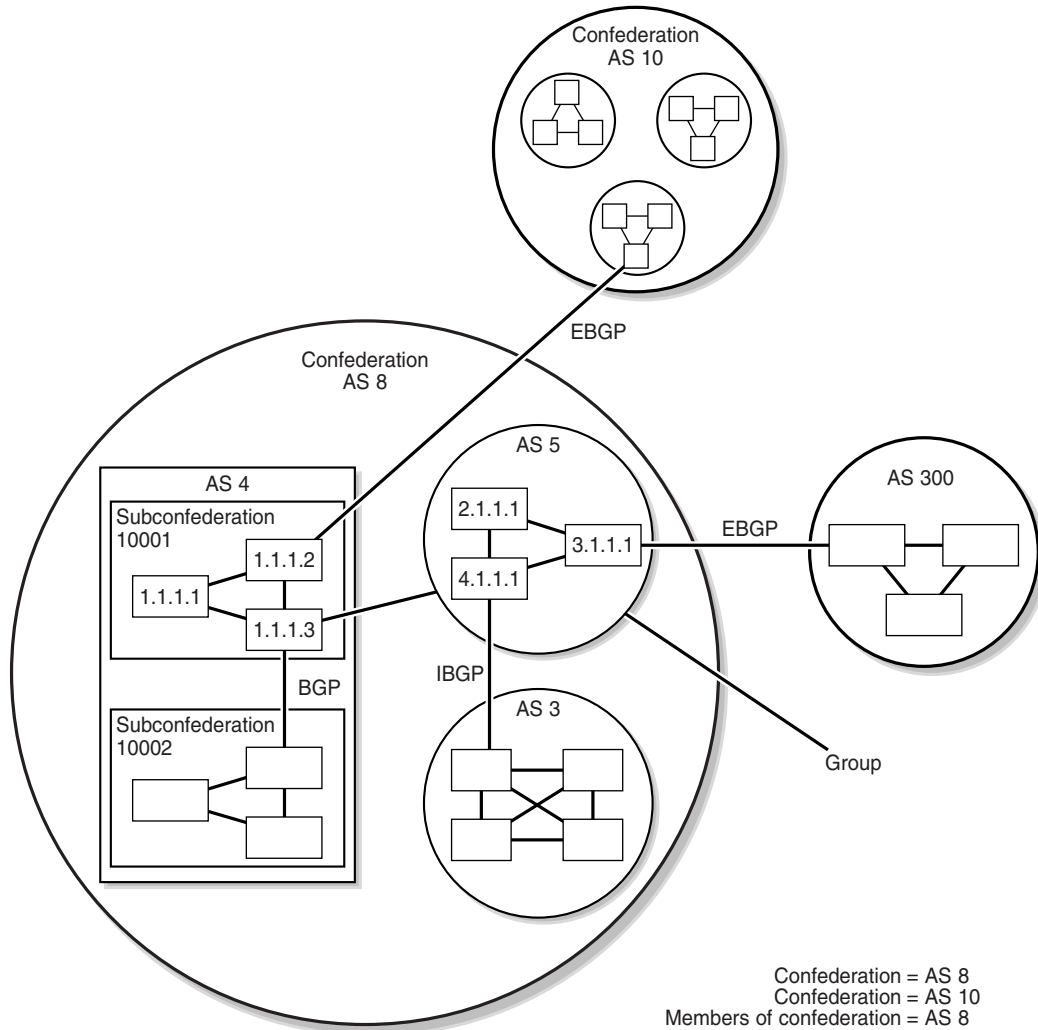
You can use the 5620 SAM to enable BGP on the device and configure:

- set the AS values for the routing instance
- create confederations to group-managed devices
- create BGP peer groups
- create neighbors within the BGP peer groups

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 address of the devices that are peers of the local BGP system.

Figure 17-2 shows a simple BGP example using groups, subconfederations, and confederations.

Figure 17-2 BGP example



```

Confederation = AS 8
Confederation = AS 10
Members of confederation = AS 8
-> 5
-> 3
-> 4 = 10001
      10002
AS peers in AS 10001 = 1.1.1.1
Confederation = 1.1.1.2
Confederation = 1.1.1.3
Route reflector for AS 10001 -> 1.1.1.3
    
```

17334

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.

As BGP was designed to distribute IPv4 routing information, the addition of VPN IPv4 addresses required an extension to BGP. The extension is MP-BGP. The new addressing now includes a 12-byte address, consisting of a eight-byte RD and the four-byte IPv4 address. To use MP-BGP:

- MP-BGP must be enabled on all PE devices from the VPN tab of the BGP configuration form
- all PE devices must be connected as peers

When PE devices learn routing information from customer edge devices in an IP VPN configuration, the routing information is shared using MP-BGP. The route distinguishing eight-byte address is used to associate the new routing information with an IP VPN instance.

The PE devices then distribute the routes to the customer edge devices of all other VPNs within the IP VPN instance. Each learned route is assigned an MPLS label, which is distributed to the other devices.

When customer packets arrive at the PE device, the packets are encapsulated with the MPLS label corresponding to the learned route that matches the customer packet destination address.

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 on 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 advertising 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.

You can use the 5620 SAM to enable RIP on the device. Both RIPv1 and RIPv2 are supported on all IP interfaces, including network and access interfaces. Use the CLI for additional RIP configuration. See the *7750 SR OS Router Guide* for more information.

OSPF

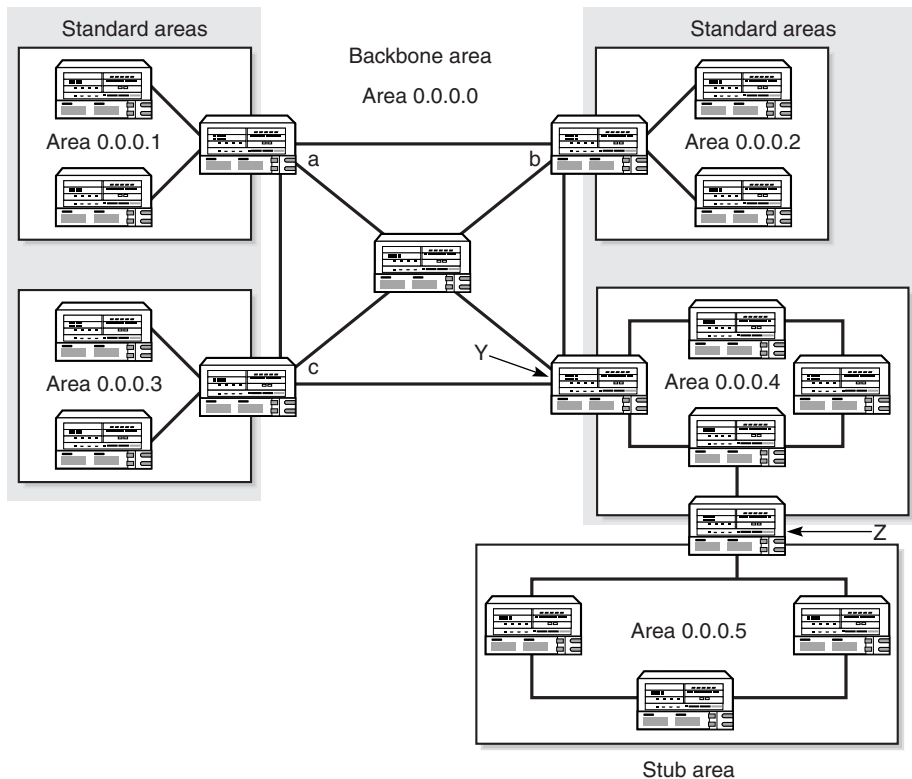
OSPF is a hierarchical link state protocol. OSPF is an IGP used within large ASs. OSPF devices exchange the state, cost, and other relevant interface information with neighbors once the neighbors are discovered. The information exchange enables all participating devices to establish a network topology map. Each device applies the Dijkstra algorithm to calculate the shortest path to each destination in the network. The resulting OSPF forwarding table is submitted to the routing table manager to calculate the routing table.

Because OSPF is hierarchical, devices are configured in logical groups called areas. The topology of each area is hidden from devices outside the area, which limits protocol traffic and routing table sizes. There are two main types of areas:

- backbone area
- standard area

Standard areas are connected to the backbone area by area border devices. Figure 17-3 shows the OSPF topology.

Figure 17-3 OSPF areas in an OSPF domain



17279

Each device in Figure 17-3 has:

- OSPF enabled on the device
- been assigned to an area
- been configured as an OSPF area device or backbone area device
- been enabled the OSPF protocol on a Layer 3 interface

You can use the 5620 SAM to configure all these OSPF settings.

When there are changes in the network, for example new neighbors are added, all devices in the appropriate areas advertise the topology changes to other devices in their area. The changes advertised only include the changes, not the entire network topology, and only the devices that need to update their routing tables do so.

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 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 will switch data accordingly.

When a service tunnel is configured to another 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:

- 1 An 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.

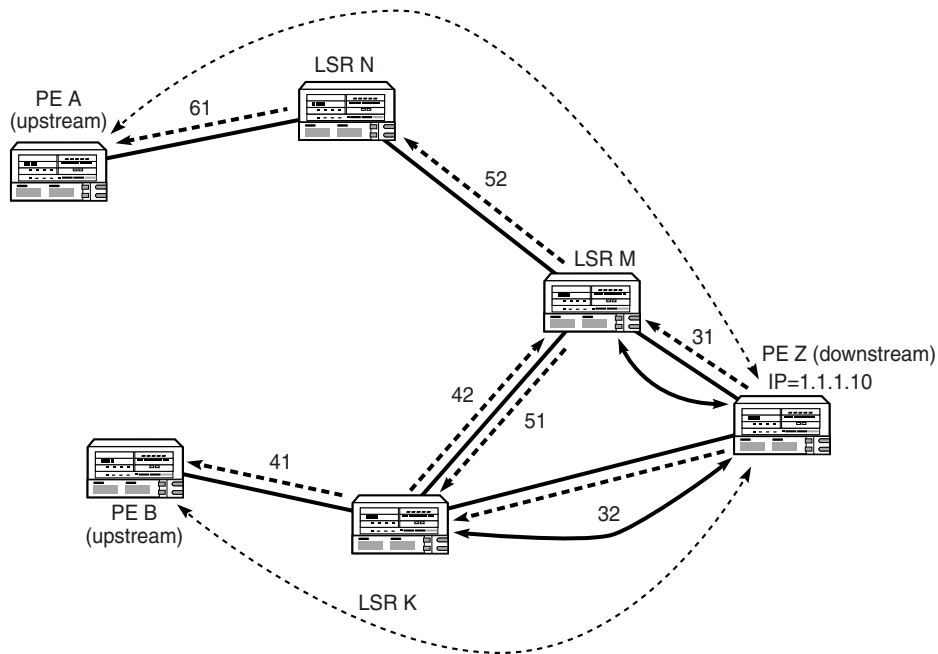
- T-LDP
- DU-LDP

T-LDP is used to distribute labels for VLL and VPLS services. 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 17-4 shows an example of LDPs that are used in a simple Layer 2 and Layer 3 service provider network.

Figure 17-4 LDP sample network



17263

- 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 the devices would have DU-LDP sessions.

Provider edge router Z advertises the labels for its address 1.1.10/32 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.

ISIS

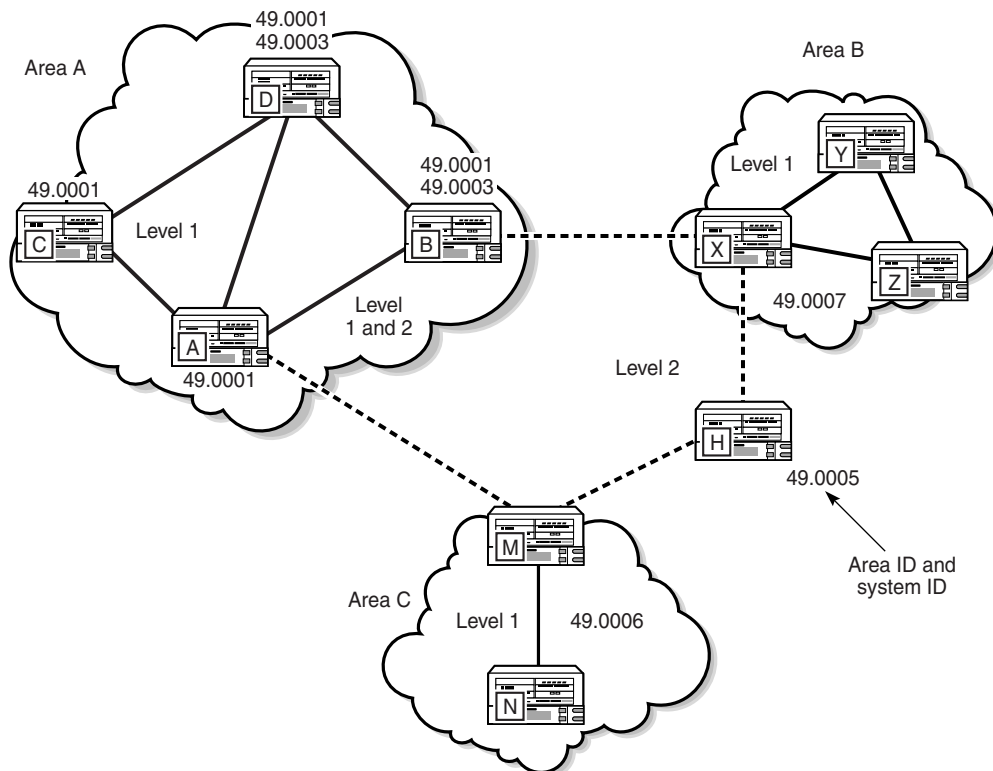
ISIS is a link-state interior gateway protocol that uses the shortest path first algorithm to determine a route. Routing decisions are made using the link-state information. ISIS entities include:

- networks, which are autonomous system routing domains
- intermediate systems, which are routers, such as the 7750 SRs
- 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 ISIS 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 ISIS 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 17-5.

Figure 17-5 ISIS routing domains example



17262

Level 2 areas are also called backbones. 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 ISIS backbone. The connection between routers A and B carries both level 1 and level 2 link-state PDUs.

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.



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.

After the ISIS is configured, routing occurs as follows:

- 1 Hello PDUs are sent to ISIS-enabled interfaces to discover neighbors and establish adjacencies.
- 2 ISIS 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 ISIS and the routing table is built.

17.2 Workflow to configure routing protocols

- 1 Prior to configuring OSPF or BGP, the router ID must be available. The router ID is a 32-bit number assigned to each router running OSPF or BGP.
- 2 Prior to configuring BGP, an autonomous system number must be assigned to the device from the Routing tab of the Routing Instance configuration form.
- 3 Enable the routing protocols to be supported on devices. The options are:
 - LDP
 - ISIS
 - MPLS
 - RSVP (enabled by default)
 - BGP
 - RIP
 - OSPF
- 4 Ensure the parameters to implement routing protocols on the Layer 3 interfaces are configured as needed. See chapter 16 for more information.
- 5 Configure routing policies for those routing protocols that use policies.
- 6 The procedures to follow depend on the type of routing protocols that you want to configure. See Table 17-1 for more information.
 - a For BGP:
 - i Determine whether BGP confederations are necessary. If BGP confederations are necessary:
 - Configure the Confederation Autonomous System number on the Routing tab of the Routing Instance configuration form.
 - Configure BGP confederation members from the BGP Confederations tab of the Routing Instance configuration form.
 - ii For MP-BGP, enable VPN IPv4 from the VPN tab button on the BGP configuration form.
 - iii Create at least one BGP peer group.
 - iv Create a BGP neighbor with which to peer.
 - v Create a BGP peer autonomous system that is associated with the neighbor peer.

- b** For RIP:
 - i** Configure global-level RIP parameters.
 - ii** Configure group-level RIP parameters.
 - iii** Configure neighbor-level (also known as interface) RIP parameters.
 - c** For OSPF:
 - i** Create at least one OSPF area.
 - ii** Assign routers to the OSPF area.
 - iii** Assign Layer 3 interfaces to the routers in the OSPF area.
 - d** For LDP:
 - i** Configure global-level LDP parameters.
 - ii** Create LDP interfaces for LDPs between adjacent devices (directly connected peers).
 - iii** Create LDP targeted peers for LDPs between non-adjacent devices (non directly connected peers).
 - e** For ISIS:
 - i** Configure global-level ISIS parameters.
 - ii** Configure at least one NET address.
 - iii** Configure at least one ISIS interface.
 - iv** Configure an operational LSP between routers.
- 7 Configure the protocol for the remote device, if applicable.

17.3 Routing protocol configuration menus

To configure routing protocols, you select the Network tab, ISIS tab, or the OSPF tab on the navigation tree. You then use the contextual menus to configure or modify the network objects.

17.4 Routing protocol configuration procedures list

Table 17-1 lists the procedures to configure routing protocols.

Table 17-1 Routing protocols configuration procedures list

Protocol	Procedure	Reference
BGP	To enable BGP on a router	See “BGP” in section 17.5 for more information.
	To configure a BGP confederation	
	To configure global-level BGP	
	To configure peer group-level BGP	
	To configure peer-level BGP	
RIP	To configure global-level RIP	See “RIP” in section 17.5 for more information.
	To configure group-level RIP	
	To configure interface-level RIP	
OSPF	To enable OSPF on a router	See “OSPF” in section 17.5 for more information.
	To configure OSPF on a router	
	To configure an OSPF area and add Layer 3 interfaces to the area	
	To add a router to an OSPF area	
	To create a virtual link	
LDP	To enable LDP on a router	See “LDP” in section 17.5 for more information.
	To configure global-level LDP parameters	
	To configure LDP interfaces	
	To configure LDP targeted peers	
ISIS	To enable ISIS	See “ISIS” in section 17.5 for more information.
	To configure ISIS parameters	
	Configure ISIS NET addresses	
	To configure ISIS interfaces	

17.5 Routing protocol configuration procedures

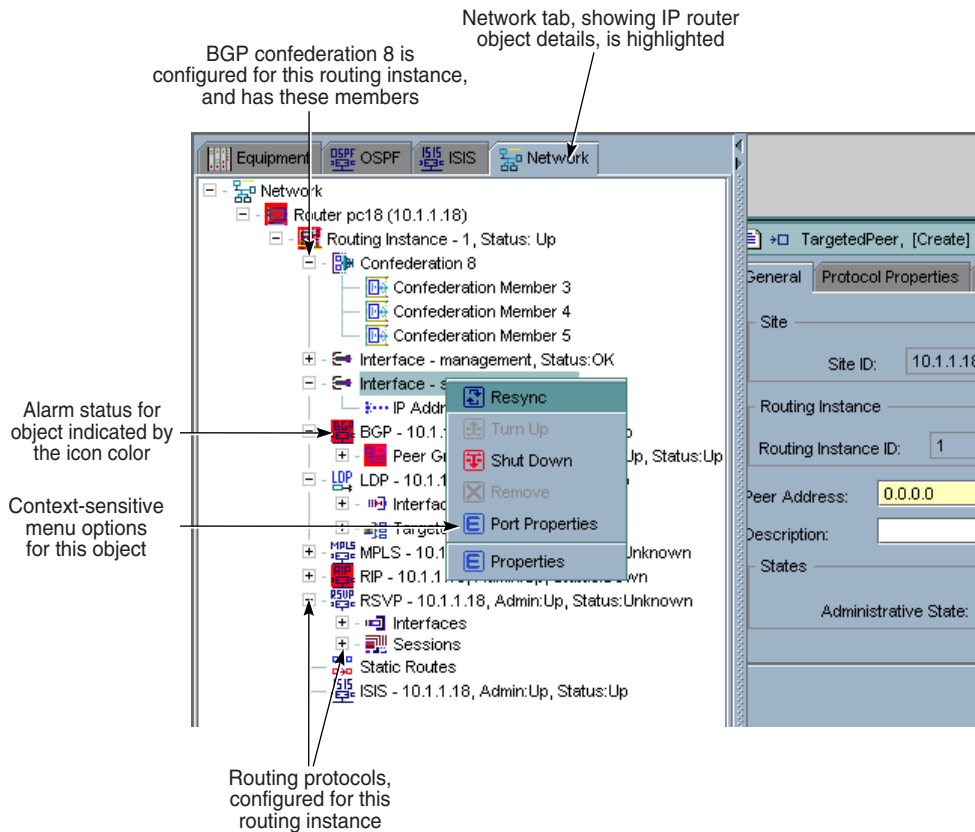
Perform the appropriate procedures for the routing protocols you want to configure. See the *7750 SR OS Router Guide* for more detailed information about routing protocol parameters.

BGP

The BGP command hierarchy consists of three levels:

- global
- peer group
- peer (also known as neighbor)

Figure 17-6 shows the Network tab open to show Confederations and BGP settings.

Figure 17-6 BGP in the navigation tree Network tab

17336

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.

Procedure 17-1 To enable BGP on a router

- 1 From the 5620 SAM GUI, select the Network tab on the navigation tree.
- 2 Navigate to the routing instance icon.
The navigation path is Network→Router→Routing Instance.
- 3 Right-click on the routing instance icon and choose Properties from the contextual menu. The Routing Instance configuration form appears.

- 4 Enable BGP.
 - i Click on the Protocols tab button.
 - ii Select the BGP Enabled check box.



Note 1 — You must configure an AS number before enabling BGP. Configure an AS number from the Routing tab on the Routing Instance configuration form.

Note 2 — If confederations are required, configure a number for the Confederation Autonomous System parameter from the Routing tab on the Routing Instance configuration form.

- 5 Click on the Apply button to save the changes.

BGP is listed in the configuration form of configured protocols and the BGP icon appears in the navigation tree under the Network tab.

Procedure 17-2 To configure global-level BGP

- 1 From the 5620 SAM GUI, select the Network tab on the navigation tree.
- 2 Navigate to the BGP icon.

The navigation path is Network→Router→Routing Instance→BGP.
- 3 Right-click on the BGP icon and choose Properties from the contextual menu.

The BGP configuration form appears.
- 4 Configure the BGP parameters. Figure 17-1 shows the BGP configuration form.

Table 17-2 describes the tabs and parameters.

Table 17-2 Global-level BGP configuration form tabs and parameters

Tab	Description
General	Configure a description of the BGP configuration, and set the administrative state to Up.
Behavior	Configure the BGP route parameters including damping, route reflection, and AS path usage. <ul style="list-style-type: none"> • The Cluster ID parameter specifies the cluster ID for a route reflector server, used to reduce the number of IBGP sessions within an AS. • The Preference parameter specifies the route preference for routes that are learned from a configured peer. The lower the preference number, the higher the chance that the route is the active route. • The AS Path Ignore parameter specifies whether the AS path is used to determine the optimum BGP route. • The Damping parameter is used to reduce the number of update messages sent between BGP peers for learned routes, as defined in the route policy.

(1 of 3)

Tab	Description
Time	Configure the Connect Retry Time, Hold Time, and Keep Alive parameters, in seconds. These parameters specify how the duration and closeout of BGP sessions are handled.
AS Properties	Configure AS parameters. The AS properties specifies the AS information that is advertised to peers. Some parameters are read-only. 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. Now RTA can advertise AS1 for routes advertised to CR1.
MultiPath	Configure multipath parameters. <ul style="list-style-type: none"> When the MultiPath parameter is set to 1, multipath is disabled. When the MultiPath parameter is set to 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. When the IGBP MultiPath parameter is set to true, the type of IGBP used to resolve BGP next hop issues when two or more equally valid next hops are available.
MED	Configure parameters to advertise the MED. These parameters are used to find a way to exit the AS when there are multiple methods of leaving the AS. <ul style="list-style-type: none"> The MED Compare parameter specifies how the MED operates in the BGP route selection process. When the parameter is set to zero, it specifies that, for routes learned without a MED parameter, 0 is used in the MED comparison. This helps make a 0 MED path a more desirable route. When the parameter is set to infinity, it specifies that infinity is used in the MED comparison. This helps make an infinity MED path a less desirable route. The MED Source parameter enables advertisement of the MED value to BGP peers. When the parameter is set to none, no MED value is advertised. When the parameter is set to IGP cost, the MED is set to the IGP cost. When the parameter is set to Metric Value, a number up to infinity must be configured. This is the MED value.
VPN	Configure VPN parameters, including: <ul style="list-style-type: none"> the Family parameter to specify the type of VPN, which is VPN IPv4 (used for route distinguishing for IP VPN services to enable MP-BGP) or IPv4 whether to apply the existing import and export route policies configured on the Import Policies and Export Policies tabs
Group	Configuration of the BGP peer groups is optional. To configure groups, click on the Add button and configure the parameters, or choose the BGP icon and choose Create Group from the contextual menu. See Procedure 17-4 for more information.
Peer	Configuration is not required. To configure peers, click on the Add button and configure the parameters, or choose the BGP icon and choose Create Peer from the contextual menu. See Procedure 17-5 for more information.
Import Policies	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 16. There is no validation performed by the router to ensure the policies match.
Export Policies	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 16. There is no validation performed by the router to ensure the policies match.

(2 of 3)

Tab	Description
Authentication	Configure the parameters that enable MD5 authentication and the authentication key to authenticate neighboring routers before a BPG session is set up. <ul style="list-style-type: none"> The Type parameter specifies the type of authentication, which is MD5 or none. The key parameter specifies the MD5 authentication key used by the routers to authenticate each other.
Statistics	View statistics per BGP.
Faults	View alarms raised against BGP, or to view alarms raised against objects that affect BGP.

(3 of 3)

- 5 Click on the Apply button to save the changes.
- 6 Click on the OK button.

Procedure 17-3 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 17-1 and 17-2.

- 1 From the 5620 SAM GUI, select the Network tab on the navigation tree.
- 2 Navigate to the routing instance icon.
The navigation path is Network→Router→Routing Instance.
- 3 Right-click on the Routing Instance icon and choose Properties from the contextual menu.
The Routing Instance configuration form appears.
- 4 Click on the Routing tab button.
- 5 Enter the confederation number for the Confederation Autonomous System parameter.
- 6 Click on the BGP Confederations tab button.
- 7 Click on the Add button to add a BGP confederation, or click on the Edit button to configure an existing BGP confederation. The Confederation Routing Instance form appears.

You can only have one BGP confederation for each device.

- 8 From the General tab of the Confederation Routing Instance, you can view the Confederation Autonomous System number. Figure 17-7 shows the confederation form for the routing instance with the General tab button selected.

Figure 17-7 Routing instance confederation form - General

The screenshot shows a configuration window titled "Confederation - 8, Routing Instance - 1, 10.1.1.18 [Edit]". It has three tabs: "General", "Members", and "Faults", with "General" selected. The form contains the following fields:

- Site:** Site ID: 10.1.1.18, Site Name: pc18
- Routing Instance:** Routing Instance ID: 1, Routing Instance Name: Base
- Confederation AS:** 8

At the bottom of the window, there are buttons for "Copy...", "Resync", "Reset", "OK", "Cancel", and "Apply".

To add new members to the confederation:

- i Click on the Members tab button.
- ii Click on the Add button. The Confederation Member configuration form appears. Figure 17-8 shows the confederation member configuration form with the General tab button selected.

Figure 17-8 Confederation member form - General

The screenshot shows a configuration dialog box titled "Confederation Member - 3, Confederation - 8, Routing Instance - 1, 10.1.1.18 [Edit]". It has two tabs: "General" and "Faults". The "General" tab is active and contains the following fields:

- Site:** Site ID: 10.1.1.18, Site Name: pc18
- Routing Instance:** Routing Instance ID: 1, Routing Instance Name: Base
- Confederation AS:** 8, **Member AS:** 3

At the bottom of the dialog, there are several buttons: "Copy...", "Resync", "Remove" (with a red X icon), "Reset", "OK", "Cancel", and "Apply".

- iii Specify 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 Apply button to save the changes.

A row is added to the list of confederation members, which indicates that the AS that is in the confederation.

- v Repeat for each AS that you want in the confederation by specifying the Member AS parameter.
- 9 Click on the Apply button. The Confederation icon appears in the Navigation Tree below the Routing Instance icon.

Verify the confederation membership by opening the Confederation icon to view an icon that represents each member of the confederation, as specified in step 8.

From the Fault tab, you can view alarms raised against confederation members ASs, or faults raised against the confederation itself.

After the confederation is created, right-click on the confederation or the confederation member icons to perform maintenance tasks using the contextual menu:

- Resync to resynchronize the network management settings with the device
- Copy to create a member AS based on the existing configuration settings of the chosen object
- Properties to view the configuration settings
- Remove to remove a member AS from the confederation

Procedure 17-4 To configure peer group-level BGP

- 1 From the 5620 SAM, select the Network tab on the navigation tree.
- 2 Navigate to the BGP icon.
The navigation path is Network→Router→Routing Instance→BGP.
- 3 Right-click on the BGP icon and choose Create Group from the contextual menu.
The Peer Group configuration form appears.
- 4 Configure the BGP peer group parameters.
 - i Specify the name.
 - ii Click on the Behavior tab button.
 - iii Specify the Local Address and the Prefix Limit parameters.
 - iv Click on the AS Properties tab button.
 - v Specify the Peer AS parameter for this specific group, and the behavior, either internal or external. Multipath configurations are not supported at the BGP peer level.
 - vi You can choose to inherit values from the parameters specified in Table 17-2 by checking the Inherit check box.



Note — If you choose not to inherit the value from the global-level parent BGP configuration, you can only choose the option(s) not set in the parent configuration. For example, if the Damping parameter is set to false on the global-level BGP configuration form, you can only set the Damping parameter to true on the group-level BGP.

The parameters you configure for the BGP peer group take precedence over the parameters you configure for the BGP global-level.

- 5 Click on the Apply button to save the changes.
 - 6 Click on the OK button.
-

Procedure 17-5 To configure peer-level BGP

- 1 From the 5620 SAM, select the Network tab on the navigation tree.
- 2 Navigate to a peer group.
The navigation path is Network→Router→Routing Instance→BGP→*Peer Group*, where *Peer Group* is the group that you created in Procedure 17-4.
- 3 Right-click on the peer group icon and choose Create Peer from the contextual menu.

The Peer, Peer Group configuration form appears.

- 4 Configure the peer parameters.
 - i Configure the Peer Address parameter, which is the IP address of the far-end peer that you are pointing at.
 - ii You can choose to inherit values from the parameters specified in Table 17-2 by checking the Inherit check box.



Note — If you choose not to inherit the value from the global-level parent BGP configuration, you can only choose the option(s) not set in the parent configuration. For example, if the Damping parameter is set to false on the global-level BGP configuration form, you can only set the Damping parameter to true on the peer-level BGP.

The parameters that you configure for the BGP peer (also known as the BGP neighbor) take precedence over the parameters that you configure for the BGP peer group and the BGP global-level.

- 5 Click on the Apply button to save the changes.
 - 6 Click on the OK button.
 - 7 Configure the protocol for the far-end device, if applicable. Use CLI for non-5620 SAM managed devices.
-

RIP

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.

Procedure 17-6 To configure global-level RIP

- 1 From the 5620 SAM, select the Network tab on the navigation tree.
- 2 Navigate to the RIP icon.

The navigation path is Network→Router→Routing Instance→RIP.
- 3 Right-click on the RIP icon and choose Properties from the contextual menu.

The RIP configuration form appears.

- 4 Configure the RIP parameters. Table 17-3 describes the tabs and parameters.

Table 17-3 Global-level RIP configuration form

Tab	Description
General	Configure a description of the RIP configuration, and set the administrative state to Up.
Behavior	Configure the RIP route parameters including: <ul style="list-style-type: none"> • checking for zero values in fields specified to be zero by the RIPv1 and RIPv2 specifications • message size • metrics for incoming and outgoing routes • type of messages received based on the RIP version • type of messages sent based on RIP version, and the variation of RIPv2 messages sent, either broadcast or multicast • preference of route based on cost • split-horizon with poison reverse • timers
Authentication	Configure the authentication type, and the authentication key that is passed between RIP interfaces to ensure security.
Import Policies	Choose route policies that determine the routes that are accepted from RIP interfaces. You can choose up to five route policies. The route policies are enforced in order, from one to five.
Export Policies	Choose route policies that determine the routes that are exported to RIP interfaces. You can choose up to five route policies. The route policies are enforced in order, from one to five.
Group	Configure group-level RIP parameters. Click on the Add button to add a group. See Procedure 17-7 for more information.
Interface	Configure interface-level (also known as neighbor) RIP parameters. Click on the Add button to add an interface. See Procedure 17-8 for more information.
Statistics	View statistics related to RIP.
Faults	View alarms related to RIP, or to view alarms raised against object that affect RIP.

Procedure 17-7 To configure group-level RIP

- 1 From the 5620 SAM, select the Network tab on the navigation tree.
- 2 Navigate to the RIP icon.

The navigation path is Network→Router→Routing Instance→RIP.
- 3 Right-click on the RIP icon and choose Create Group from the contextual menu.

The RIP Group configuration form appears.
- 4 Specify a name for the RIP group.
- 5 Configure the RIP group parameters, as listed in Table 17-3.

You can choose to inherit values from the parameters specified in Table 17-3 by checking the Inherit check box. The parameters that you configure for the RIP group take precedence over the parameters you configure for the RIP global-level.

- 6 Click on the Apply button to save the changes.
 - 7 Click on the OK button.
-

Procedure 17-8 To configure interface-level RIP

- 1 From the 5620 SAM, select the Network tab on the navigation tree.
 - 2 Navigate to an RIP group.

The navigation path is Network→Router→Routing Instance→RIP→*RIP Group*,
where *RIP Group* is the group you created in Procedure 17-7
 - 3 Right-click on the RIP group icon and choose Create Interface from the contextual menu.

The Interface, RIP Group configuration form appears.
 - 4 Configure the interface-level RIP parameters, as listed in Table 17-3.

You can choose to inherit values from the parameters specified in Table 17-3 by checking the Inherit check box. The parameters that you configure for the RIP interface (also known as the RIP neighbor) take precedence over the parameters that you configure for the RIP group- and global-level parameters.
 - 5 Click on the Apply button to save the changes.
 - 6 Click on the OK button.
-

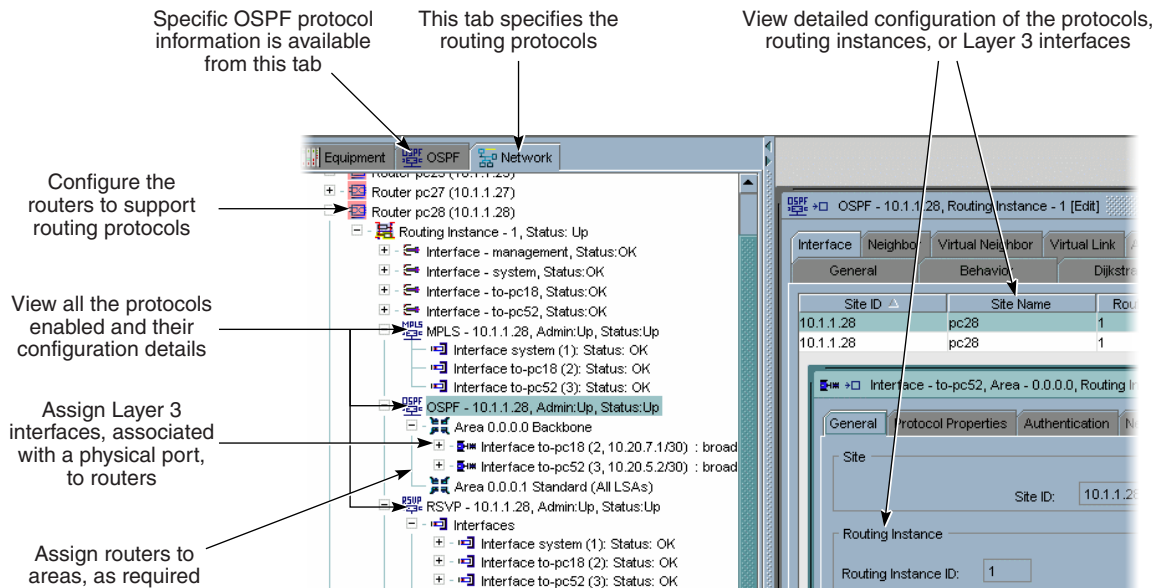
OSPF

Configuration planning is essential to organize devices, backbone, non-backbone, stub, NSSA areas, and transit links. OSPF provides defaults for basic protocol operability. At a minimum:

- Create a single OSPF backbone area which contain the area border routers.
- For larger networks, create several areas containing the other routers.
- For smaller networks, place all routers in the OSPF backbone area.

Use the 5620 SAM to configure the OSPF parameters. Figure 17-9 shows the OSPF tab in the navigation tree.

Figure 17-9 OSPF tab



17281

The OSPF parameters that must be configured to deploy OSPF are:

- Router ID — Each device that runs OSPF must be configured with a unique router ID. The router ID is used by both 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 associated with it, which is obtained from the underlying lower-level protocols and the routing protocol. An interface to a network has an associated IP address and mask (unless the network is an unnumbered, point-to-point network). An interface is sometimes also referred to as a link or a routing instance.

Procedure 17-9 To enable OSPF on a router

- 1 From the 5620 SAM GUI, select the Network tab on the navigation tree.
- 2 Navigate to the routing instance icon.
The navigation path is Network→Router→Routing Instance.
- 3 Right-click on the routing instance icon and choose Properties from the contextual menu.

The Routing Instance configuration form appears.

- 4 Enable OSPF.
 - i Click on the Protocols tab button.
 - ii Select the OSPF Enabled check box.
- 5 Click on the Apply button to save the changes.

The OSPF is listed in the configuration form of configured protocols and the OSPF icon appears in the navigation tree under the Network tab.

Procedure 17-10 To configure OSPF on a router

- 1 From the 5620 SAM GUI, select the Network tab on the navigation tree.
- 2 Navigate to the OSPF icon.

The navigation path is Network→Router→Routing Instance→OSPF.
- 3 Right-click on the OSPF icon and choose Properties from the contextual menu. The OSPF configuration form appears.
- 4 Configure the OSPF parameters. Figure 17-10 shows the OSPF configuration form with the General tab button selected.

Figure 17-10 OSPF configuration form - General

The screenshot displays the OSPF configuration form for a routing instance named 'Base'. The 'General' tab is selected, showing the following parameters:

- Site:** Site ID: 10.1.1.23, Site Name: pc23
- Routing Instance:** Routing Instance ID: 1, Routing Instance Name: Base, OSPF Router ID: 10.1.1.23
- Type:** IP Address, in the form xxx.xxx.xxx.xxx. Checkboxes for Area Border Router, Autonomous System Border Router, and Backbone Router are all unchecked.
- State:** Administrative State: Up, Operational State: Up, Last Time Enabled: 01/01/1970 02:05:39 560 EST

Buttons at the bottom include Resync, Turn Up, Shut Down, Reset, OK, Cancel, and Apply.

Table 17-4 describes the tabs and parameters.

Table 17-4 OSPF configuration form tabs and parameters

Tab	Description
General	Specify the router as an ASBR, and to set the administrative state to Up. You can also view the routing instance used or router information.
Behavior	Configure the parameters for traffic engineering, RFC compatibility, aging, overflow control, preferences, and LSAs.
Dijkstra	Configure the timers that control the delay between the receipt of LSAs that require Dijkstra shortest path first calculation.
Export Policies	Configure the export route policy used to determine which routes are advertised to peers.
Area Site	Configuration of the area site is optional. Click on the Add button to configure an area for the routing instance, or click on the Edit button to modify the configuration of an existing area: <ul style="list-style-type: none"> Specify the type of area, either backbone, stub, or NSSA. Specify an ID for the area. Select the Blackhole Range check box to enable the blackhole range. See Procedure 17-11 for more information.
Interface	Configuration of the interface is optional.
Neighbor	Read-only
Virtual Neighbor	Read-only
Virtual Link	Configuration of the virtual link is optional.
Area Range	Configuration is optional.
Statistics	View statistics related to OSPF.
Faults	View alarms raised against OSPF, or to view alarms raised against objects that affect OSPF.

- 5 Click on the Apply button to save the changes.
- 6 Click on the OK button.

Procedure 17-11 To configure an OSPF area and add Layer 3 interfaces to the area

You must create at least one OSPF area.

- 1 From the 5620 SAM, select the OSPF tab on the navigation tree.
- 2 Select the network icon.
- 3 Right-click and choose Create Area from the contextual menu.
The Area (Create) configuration form appears.
- 4 Associate a routing instance on the router and add it to the area.
- 5 Give the area a name and description.

- 6** Configure the area ID to define the OSPF area. The number is a 32-bit hexadecimal number in the form of an IP address or a single digit number to imply 0.0.0.x, where x identifies the area.
- 7** Choose the type of area to configure. The Type parameter options are:
 - Backbone
 - Standard (All LSAs) (default)
 - Stub (No Type 5 External)
 - Totally Stub (No Summaries)
 - NSSA (No Type 5 External)
 - NSSA (No Summaries)
- 8** Click on the OK button to save the changes.

The 5620 SAM updates the navigation tree to display the area that you have created.
- 9** Open an area icon.

The routers belonging to the area are displayed.
- 10** Choose a router added to the area.
- 11** Right-click on the router icon and choose Create Interface from the contextual menu. This action will assign an existing Layer 3 interface, rather than create a new Layer 3 interface.

The Interface Area configuration form appears.
- 12** From the General tab, click on the Select button next to the Interface Name parameter.

The Select Locale form appears.
- 13** Specify the Locale as either Access or Network.
- 14** Click on the OK button.
- 15** Use the filter options to generate a list of interfaces, if required, and click on the OK button.

The list of available Layer 3 interfaces appears.
- 16** Choose a Layer 3 interface from the list and click on the OK button.

The Layer 3 interface is added.
- 17** Click on the Protocol Properties tab.
- 18** Configure the Layer 3 interface protocol parameters, such as the:
 - type of OSPF used
 - hello and polling intervals
 - priority
 - Type parameter to broadcast to create a broadcast interface. Set to Point to Point to create an PPP interface.

- 19 Click on the OK button.

The Layer 3 interface is added to the router in the area.

The router will now begin to attempt reaching neighboring routers that may be connected on the interface. The routers will recognize links to the neighboring routers and share OSPF routing information.

Once this is complete, neighbor information appears in the navigation tree under the Layer 3 interface icon.

- 20 Configure the area that you created, select the area icon from the navigation tree.



Note — To view area information, a router must be added to the area. See Procedure 17-12 to add a router to an OSPF area.

- 21 Right-click and choose Properties from the contextual menu.

The 5620 SAM displays the Area configuration form. Figure 17-11 shows the configuration form for a Standard (All LSAs) OSPF area with the General tab button selected.

Figure 17-11 OSPF area form - General

The screenshot shows a configuration window titled "Area - 0.0.0.56 [Edit]". The window has several tabs: "General", "Area Site", "Interface", "Virtual Link", "Area Range", and "Faults". The "General" tab is active. The form contains the following fields and controls:

- ID:** Text box containing "0.0.0.56"
- Name:** Text box containing "0.0.0.56"
- Type:** Dropdown menu set to "Standard (All LSAs)"
- Type Mismatch:** An unchecked checkbox
- Description:** Text box containing "N/A"

At the bottom of the window, there is a row of buttons: "Resync", "New...", "Copy...", "Reset", "OK", "Cancel", and "Apply".

- 22** Configure the OSPF area parameters. Table 17-5 describes the tabs and parameters.

Table 17-5 OSPF area configuration form tabs and parameters

Tab	Description
General	Reconfigure the type of area, and to enable the area as a blackhole range to avoid routing loops.
Area Site	Display the routers that are assigned to the OSPF area.
Stub/NSSA	Configure the NSSA and stub parameters. This tab appears for stub, totally stub, and NSSA areas. For all other areas, the tab is dimmed.
Interface	All the Layer 3 interfaces are listed. Click on the Add button to open the Layer 3 interface configuration form. You must assign a Layer 3 interface to each OSPF area.
Virtual Link	Click on the Add button to open the virtual link configuration form. Virtual links are used to link remote areas that do not advertise their OSPF topology.
Area Range	Click on the Add button to configure the area range. The area range minimizes the advertisements that are flooded by summarizing a range of IP addresses in an LSA.
Faults	View alarms raised against OSPF areas, or to view alarms raised against objects that affect OSPF areas.

- 23** Click on the Apply button to save the changes.

- 24** Click on the OK button.

Procedure 17-12 To add a router to an OSPF area

- 1** From the 5620 SAM, select the OSPF tab on the navigation tree.
- 2** Navigate to the area in which you want to add routers.
- 3** Right-click on the area icon and choose Add Router from the contextual menu.

The 5620 SAM displays the Area configuration form. Figure 17-12 shows the Area configuration form from which you choose a router to add.

Figure 17-12 Area configuration form - General

- 4 Click on the Select button next to the Routing Instance Name parameter to choose the routing instance to add.

The Select Routing Instance form appears.

- 5 Choose a routing instance from the list.
- 6 Click on the OK button.

The routing instance is added to the Routing Instance Name parameter.

- 7 Set the Stub and NSSA parameters when adding routers to the stub or NSSA OSPF areas.

For NSSA, choose whether to perform distribution of external routes. If you choose to distribute then distribute external routes, and set the default cost.

- 8 Click on the Apply button to save the changes.
- 9 Click on the OK button.

The router appears in the area.

- 10 Right-click on the router icon and choose Create Interface from the contextual menu.

The Interface Area configuration form appears.

- 11 Follow steps 12 in Procedure 17-11 to the end of Procedure 17-11 to associate the Layer 3 interfaces and area properties.

Procedure 17-13 To create a virtual link

- 1 From the 5620 SAM, select the OSPF tab on the navigation tree.
 - 2 Navigate to the area in which you want to add routers.
 - 3 Right-click on the area icon and choose Create Virtual Link from the contextual menu.

The 5620 SAM displays the Virtual Link (Create) configuration form.
 - 4 Specify the Virtual Neighbor Router (Site) ID and Transit Area parameters.
 - 5 Click on the Protocol Properties tab button.
 - 6 Specify the OSPF virtual link hello interval parameters.
 - 7 Click on the Apply button.
 - 8 Click on the OK button.
-

LDP

T-LDP is supported on 7750 SRs and 7450 ESSs, DU-LDP and LDP are only supported on the 7750 SR.

From the Network tab routing instance, there are two trees for LDP: Interfaces and Targeted LDP Peers.

The Interfaces tree lists all the configured LDP interfaces for directly connected peers. As shown in Figure 17-4, there are 2 LDP interfaces for PE Z.

The Targeted LDP tree lists indirect peers. As shown in Figure 17-4, PE A and PE B are indirect peers.

Procedure 17-14 To enable LDP on a router

- 1 From the 5620 SAM GUI, select the Network tab on the navigation tree.
- 2 Navigate to the routing instance icon.

The navigation path is Network→Router→Routing Instance.
- 3 Right-click on the routing instance icon and choose Properties from the contextual menu.

The Routing Instance configuration form appears.
- 4 Enable LDP.
 - i Click on the Protocols tab button.
 - ii Select the LDP Enabled check box.

LDP is listed in the configuration form of configured protocols and the LDP icon appears in the navigation tree.

- 5 Click on the Apply button to save the changes.

Procedure 17-15 To configure global-level LDP parameters

- 1 Enable LDP on the router, as described in Procedure 17-14.
- 2 You can:
 - a Select LDP from the list of protocols on the Routing Instance configuration form and click on the Edit button.
 - b Click on the LDP icon in the navigation tree. Choose Properties from the contextual menu.

The navigation path is Network→Router→Routing Instance→LDP.
- 3 The LDP (Edit) configuration form appears, as shown in Figure 17-13. The figure shows an LDP configuration form with the Interface Properties tab button selected.

Figure 17-13 LDP configuration form - Interface Properties

The screenshot shows a configuration window titled "LDP - 10.1.1.23, Routing Instance - 1 [Edit]". The "Interface Properties" tab is selected. The form contains the following fields and values:

- De-aggregate FEC:
- Route Preference:
- Address Type: - Propagate Policy:
- Timer Control section:
 - Keep Alive Factor: Keep Alive Timeout:
 - Hello Factor: Hello Timeout:

At the bottom of the window, there are buttons for "Resync", "Reset", "OK", "Cancel", and "Apply".

- 4 Configure the LDP parameters. Table 17-6 describes the tabs and parameters.

Table 17-6 Global-level LDP configuration form tabs and parameters

Tab	Description
General	Set the administrative state to Up to enable LDP on the device.
Common	<p>Configure and view information about the LDP on the router:</p> <ul style="list-style-type: none"> • The LSR ID is the ID of the router as a label switched router. • The distribution mode displays the method used to distribute labels. • The remaining values are determined by the router settings. <p>Set the Targeted Sessions Allowed parameter to true to configure the router for T-LDP. Targeted sessions are LDP sessions between non-directly connected peers to distribute labels.</p>
Interface Properties	<p>Configure and view information about the LDP interfaces and how the device communicates with directly connected peers. By default, the parameter values are inherited by all LDP interfaces.</p> <p>Both the keep alive factor and the keep alive timeout must be configured if one of them is configured. Both the hello factor and the hello timeout interval must be configured if one is configured.</p> <ul style="list-style-type: none"> • Specify the Address Type parameter as system or interface <ul style="list-style-type: none"> • Choose system to have the system IP address set up LDP sessions. • Choose interface to have the IP interface address set up LDP sessions; but it cannot be used if there are multiple interfaces between the two neighbors. • Specify the timer controls that control the LDP sessions between label switched routers. • Specify the keep alive factor, which is the number of keep alive messages that are sent on an idle LDP session between non-directly connected peers. • Specify the keep alive timeout, which is the interval, in seconds, that an LDP waits before tearing down an idle session. • Specify the hello factor, which is the number of hello messages sent in a hold time interval. • Specify the hello timeout interval, which is the interval, in seconds, that an LDP waits before declaring a neighbor to be down.
Targeted Peers Properties	<p>View and configure settings for targeted LDP peers and how the device communicates with non directly connected peers. You can use the configured information as a template for all other targeted peer configurations. By default, these parameter values are inherited by all LDP targeted peers.</p> <p>Both the keep alive factor and the keep alive timeout must be configured if one of them is configured. Both the hello factor and the hello timeout interval must be configured if one of them is configured.</p> <ul style="list-style-type: none"> • Specify the keep alive factor, which is the number of keep alive messages that are sent on an idle LDP session between non-directly connected peers. • Specify the keep alive timeout, which is the interval, in seconds, that an LDP waits before tearing down an idle session. • Specify the hello factor, which is the number of hello messages sent in a hold time interval. • Specify the hello timeout interval, which is the interval, in seconds, that an LDP waits before declaring a neighbor to be down.
Interfaces	A list of interfaces you can view or configure. See Procedure 17-16 for more information about configuring LDP interfaces.
Targeted Peers	A list of targeted peers you can view or configure. See Procedure 17-17 for more information about creating targeted peers.
Sessions	The list of LDP sessions shows a representation and information of the active LDP communication sessions between interfaces and targeted peers between the routers running LDP.

(1 of 2)

Tab	Description
Authentication	Configure the authentication parameters to specify the MD5 key or password to verify PDUs sent by neighboring routers on the interface. You can specify password or MD5 key authentication, and the appropriate password string or key. Click on the Add button. The MD5key configuration form appears. Configure the IP address of the remote peer. Enter the MD5 password key.
Statistics	View statistics related to LDPs.
Faults	View alarms raised against LDPs, or to view alarms raised against objects that affect LDPs.

(2 of 2)

- 5 Click on the Apply button to save the changes.

Procedure 17-16 To configure LDP interfaces

- 1 From the 5620 SAM GUI, select the Network tab on the navigation tree.
- 2 Navigate to an LDP interface.

The navigation path is Network→Router→Routing Instance→LDP→Interfaces→*Interface name*.
- 3 Right-click on the *Interface name* icon and choose Properties from the contextual menu.

The Interface configuration form appears.
- 4 Configure the interface parameters by clicking on the appropriate tab and configuring the parameters. Table 17-7 describes the tabs and parameters.

Table 17-7 LDP interface configuration form tabs and parameters

Tab	Description
General	Configure a description of the LDP interface configuration, and set the administrative state to Up to enable the LDP interface on the device. Create the interface by clicking on the Select button. Choose a Layer 3 interface from the Select Interface form.
Protocol Properties	View and configure the settings for targeted LDP peers. You can use the configured information as a template for other targeted peer configurations. You can inherit the value(s) from the global-level LDP configuration settings, or you can select the check mark in the inherit value box next to each parameter, and reconfigure the parameters specifically for the targeted peer. Both the keep alive factor and the keep alive timeout must be configured if one of them is configured. Both the hello factor and the hello timeout interval must be configured if one of them is configured. <ul style="list-style-type: none"> • Specify the keep alive factor, which is the number of keep alive messages that are sent on an idle LDP session between non-directly connected peers. • Specify the keep alive timeout, which is the interval, in seconds, that an LDP waits before tearing down an idle session. • Specify the hello factor, which is the number of hello messages sent in a hold time interval. • Specify the hello timeout interval, which is the interval, in seconds, that an LDP waits before declaring a neighbor to be down.
Statistics	View statistics related to LDP interfaces.
Faults	View alarms raised against LDP interfaces, or to view alarms raised against objects that affect LDP interfaces.

5 Click on the Apply button to save the changes.

6 Click on the OK button.

Procedure 17-17 To configure LDP targeted peers

1 From the 5620 SAM GUI, select the Network tab on the navigation tree.

2 Navigate to an LDP interface.

The navigation path is Network→Router→Routing Instance→LDP.

3 Right-click on the LDP icon and choose Create Targeted Peer from the contextual menu. The TargetedPeer (Create) configuration form appears with the General tab button selected, as shown in Figure 17-14.

Figure 17-14 LDP targeted peer form - General

The screenshot shows a configuration window titled "TargetedPeer, [Create]". It has three tabs: "General", "Protocol Properties", and "Statistics". The "General" tab is active and contains the following fields:

- Site:** Site ID: 10.1.1.23, Site Name: pc23
- Routing Instance:** Routing Instance ID: 1, Routing Instance Name: Base
- Peer Address:** 5.6.7.8
- Description:** Description of targeted peer
- States:** Administrative State: Up (dropdown), Operational State: Unknown

At the bottom of the form are four buttons: Reset, OK, Cancel, and Apply.

- Configure the parameters. Table 17-8 lists the tabs and parameters.

Table 17-8 LDP targeted peers configuration form tabs and parameters

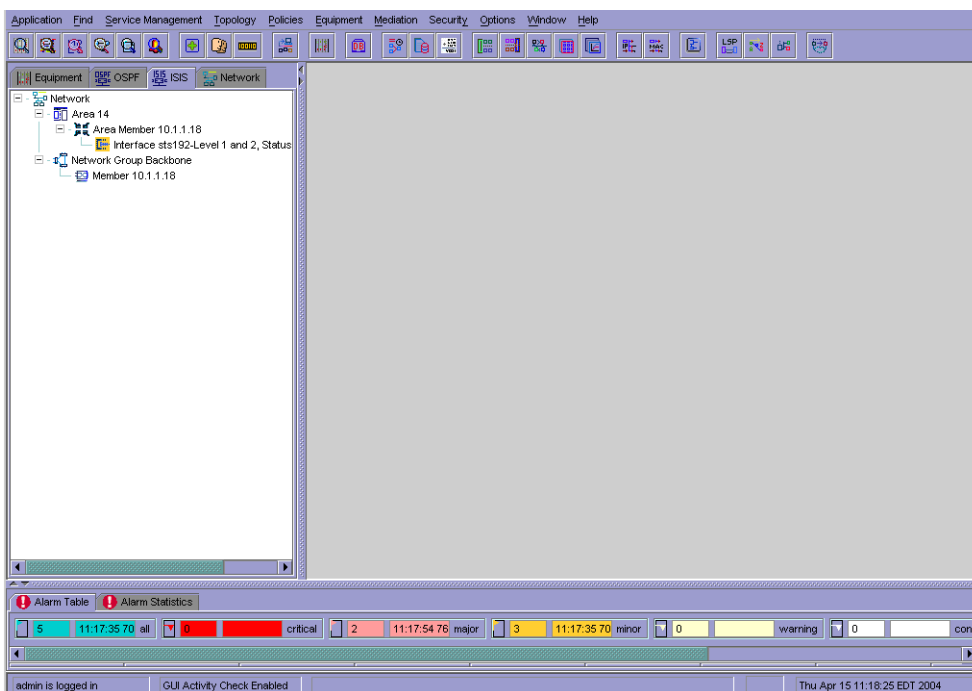
Tab	Description
General	Configure the IP address of the remote device that is the targeted LDP peer, and a description. Set the administrative state to Up.
Protocols Properties	View and configure the settings for the targeted LDP peer. You can use the configured information as a template for other targeted peer configurations. You can inherit the value from the global-level LDP configuration settings, or you can select the check mark in the inherit value box next to each parameter, and reconfigure the parameters specifically for the targeted peer. Both the keep alive factor and the keep alive timeout must be configured if one of them is configured. Both the hello factor and the hello timeout interval must be configured if one of them is configured. <ul style="list-style-type: none"> Specify the keep alive factor, which is the number of keep alive messages that are sent on an idle LDP session between non-directly connected peers. Specify the keep alive timeout, which is the interval, in seconds, that an LDP waits before tearing down an idle session. Specify the hello factor, which is the number of hello messages sent in a hold time interval. Specify the hello timeout interval, which is the interval, in seconds, that an LDP waits before declaring a neighbor to be down.
Statistics	To show statistics related to targeted LDP targeted peers.
Faults	To view alarms raised against LDP targeted peers, or to view alarms raised against objects that affect LDP targeted peers.

- Click on the Apply button to save the changes.
- Click on the OK button.
- Configure the protocol for the far-end device, if applicable. Use CLI for non-5620 SAM managed devices.

ISIS

Configuration planning is essential to organize devices in level 1, level 2 and level 1 and 2 areas. ISIS provides defaults for basic protocol operability. Use the 5620 SAM to configure the ISIS parameters. Figure 17-15 shows the ISIS tab in the navigation tree

Figure 17-15 ISIS tab



The ISIS information displayed includes:

- backbone area and the devices in the backbone area
- a list of areas and the router(s) participating in the area
- a display of devices that lists the interface IP addresses and the configured level (1, 2, or 1 and 2) of each interface

Procedure 17-18 To enable ISIS

- 1 From the 5620 SAM GUI, select the Network tab on the navigation tree.
- 2 Navigate to the routing instance icon.
The navigation path is Network→Router→Routing Instance.
- 3 Right-click on the routing instance icon and choose Properties from the contextual menu.
The Routing Instance configuration form appears.

- 4 Enable the ISIS protocol.
 - i Click on the Protocols tab.
 - ii Select the ISIS Enabled check box.
- 5 Click on the Apply button to save the changes.

ISIS is listed in the configuration form of configured protocols, the routing instance on which it is enabled, and the ISIS icon appears in the navigation tree.

Procedure 17-19 To configure ISIS parameters

Router-wide ISIS parameters can differ from the interface policies that are set in Procedure 17-21. 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 can be created between routers to exchange ISIS routing information.

- 1 Enable the ISIS protocol on a router, as described in Procedure 17-18.
- 2 You can:
 - a Choose ISIS from the list of protocols on the Routing Instance configuration form and click on the Edit button.
 - b Click on the ISIS icon in the navigation tree and choose Properties from the contextual menu.

The navigation path is Network→Router→Routing Instance→ISIS.

The ISIS routing instance form appears with the General tab button selected, as shown in Figure 17-16.

Figure 17-16 ISIS routing instance form - General

The screenshot shows the 'General' tab of the ISIS routing instance configuration form. The title bar reads 'ISIS - 10.1.200.134, Routing Instance - 1 [Edit]'. The tabs include General, Behavior, Authentication, Level 1, Level 2, Export Policies, NET Addresses, Interfaces, Statistics, and Faults. The 'General' section contains the following fields and values:

- Site ID: 10.1.200.134
- Site Name: pc134
- Routing Instance ID: 1
- Routing Instance Name: Base
- Administrative State: Up
- Operational State: Up
- System ID: 010001200134
- ISIS System Up Time: days 19:04:36 623
- Level Capability: Level 1

At the bottom of the form, there are buttons for 'Resync', 'Turn Up', 'Shut Down', 'Reset', 'OK', 'Cancel', and 'Apply'.

- 3 Configure the ISIS parameters. Table 17-9 describes the tabs and parameters.

Table 17-9 ISIS configuration form tabs

Tab	Description
General	<p>Displays read-only information about the router and routing instance.</p> <p>Set the Administrative State parameter to Up to enable ISIS.</p> <p>Configure the Level Capability parameter to Level 1, Level 2, or Level 1 and 2.</p> <p>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.</p>
Behavior	<p>The L2 to L1 Leaking parameter can be set to true to specify route leaking between levels.</p> <p>Typically, routers in level 1 only exchange information within the level 1 area. By allowing leaking between levels, domain-wide prefix distribution is enabled. This can be used to increase the granularity of routing information within the domain.</p> <p>The LSP Lifetime (seconds) parameter specifies how long the LSP is considered valid by other routers in the domain.</p>
Authentication	<p>You can enable authentication for any ISIS PDUs using the Enable Authentication parameter. The authentication parameters specify the key or password to verify PDUs sent by neighboring routers on the interface. You can specify password or MD5 authentication and the appropriate password string or key.</p>

(1 of 2)

Tab	Description
Level1	<p>From the General tab button, the External Preference and Preference (internal preference) parameters specify the route preference, which by default are as listed on the GUI. A route can be learned using different protocols:</p> <ul style="list-style-type: none"> • static route is 5 • OSPF internal route is 10 • ISIS level 1 internal route is 15 • ISIS level 2 internal route is 18 • OSPF external route is 150 • ISIS level 1 external route is 160 • ISIS level 2 external route is 165 • BGP route is 170 <p>From the Authentication tab button, configure the authentication parameters to specify the MD5 key or password to verify PDUs that are sent by neighboring routers on the interface. You can specify MD5 key or password authentication, and the appropriate password key or string.</p>
Level2	<p>From the General tab button, the External Preference and Preference (internal preference) parameters specify the route preference, which by default are as listed on the GUI. A route can be learned using different protocols:</p> <ul style="list-style-type: none"> • static route is 5 • OSPF internal route is 10 • ISIS level 1 internal route is 15 • ISIS level 2 internal route is 18 • OSPF external route is 150 • ISIS level 1 external route is 160 • ISIS level 2 external route is 165 • BGP route is 170 <p>From the Authentication tab button, configure the authentication parameters to specify the MD5 key or password to verify PDUs that are sent by neighboring routers on the interface. You can specify MD5 key or password authentication, and the appropriate password key or string.</p>
Export Policies	Specify up to five routing policies, in order of preference, to determine the routers exported from the routing table to ISIS. When multiple policies are specified, the policies are evaluated in order, from one to five.
NET addresses	See Procedure 17-20 for more information.
Interfaces	See Procedure 17-21 for more information.
Statistics	View statistics related to ISIS.
Faults	View alarms raised against ISIS, or to view alarms raised against objects that affect ISIS.

(2 of 2)

- 4 Click on the Apply button to save the changes.
- 5 Click on the OK button.

Procedure 17-20 Configure ISIS NET addresses

- 1 Enable the ISIS protocol on a device, as described in Procedure 17-18.
- 2 You can:

a Click on the NET Addresses tab on the Routing Instance configuration form.
Click on the Add button.

b Click on the ISIS icon in the navigation tree.

Choose Add NET Address from the contextual menu.

The navigation path is Network→Router→Routing Instance→ISIS.

The Area ID configuration form appears.

3 Configure the NET address used by ISIS. 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 router ID, the network service access point, and the network entity title, and from the configurable Area ID.

4 Configure the Area ID, which includes the authority and format header and the area ID.

5 Click on the OK button to save the changes.

6 Close the form.

Procedure 17-21 To configure ISIS interfaces

Interface ISIS parameters can differ from the global policies set in Procedure 17-19. Interface-level parameters specify the interface's routing levels and information. 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 ISIS routing information.

1 Enable the ISIS protocol on a router, as described in Procedure 17-18.

2 You can:

a Click on the Interfaces tab on the ISIS routing instance configuration form and click on the Add button.

b Click on the ISIS icon in the navigation tree and choose Create Interface from the right-click contextual menu.

The navigation path is Network→Router→Routing Instance→ISIS.

The Interface Routing Instance configuration form appears with the General tab button selected, as shown in Figure 17-17.

Figure 17-17 interface Routing Instance form - General

The screenshot shows a configuration window titled "Interface, Routing Instance - 1, 10.1.1.18 [Create]". It has several tabs: "General", "Behavior", "Level1", "Level2", "Authentication", and "Statistics". The "General" tab is selected. The form contains the following fields and controls:

- Site ID: 10.1.1.18 (text box)
- Site Name: pc18 (text box)
- View... (button)
- Routing Instance section:
 - Routing Instance ID: 1 (text box)
 - Routing Instance Name: Base (text box)
 - View... (button)
 - View ISIS Site (button)
- Interface section:
 - Interface ID: 0 (text box)
 - Interface Name: (text box)
 - Select... (button)
- Protocol: unknown (text box)
- Description: (text box)
- States section:
 - Administrative State: Unknown (dropdown menu)
- Capability section:
 - Type: Broadcast (dropdown menu)
 - Level Capability: Level 1 and 2 (dropdown menu)

At the bottom of the window are buttons for "Reset", "OK", "Cancel", and "Apply".

- 3 Configure the ISIS protocol interface parameters as listed in Table 17-10.

Table 17-10 ISIS protocol interface configuration form tabs and parameters

Tab	Description
General	<p>Displays read-only information about the router and routing instance.</p> <p>Set the Administrative State parameter to Up to enable the ISIS interface.</p> <p>Specify the Level Capability parameter as either Level 1, Level 2, or Level 1 and 2.</p> <p>Specify the Type parameter as Broadcast or point-to-point.</p> <ul style="list-style-type: none"> Choose Broadcast to configure the interface to maintain the link as a broadcast network. This is the default setting for IP interfaces on Ethernet ports, or for unknown port types. Choose Point-to-Point to configure the interface to maintain the link as a point-to-point link. This is the default setting for IP interfaces on SONET/SDH channels.
Behavior	<p>The Retransmit Interval (seconds) parameter specifies the minimum interval between LSP PDUs on a point-to-point interface.</p> <p>To create a mesh group, specify the same mesh group number for all interfaces, and set the Mesh Group Status parameter to Enabled. 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.</p> <p>The LSP Pacing Interval (seconds) parameter specifies the interval between LSPs being sent from the ISIS interface.</p> <p>The CSNP Interval (seconds) parameter specifies how often complete sequence number PDUs are sent from the ISIS interface. The default is five s for point-to-point interfaces. The default is 10 s for Ethernet interfaces.</p> <p>When the passive mode is enabled, the interface ignores ISIS PDUs.</p>

(1 of 2)

Tab	Description
Authentication	You can enable authentication for any ISIS 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. You can specify MD5 key or password authentication, and the appropriate password key or string.
Statistics	View statistics related to ISIS interfaces.

(2 of 2)

- 4** Click on the OK button to save the changes.
 - 5** Close the form.
-

18 — MPLS

- 18.1 MPLS configuration overview 18-2**
- 18.2 Workflow to configure MPLS 18-4**
- 18.3 MPLS menus 18-4**
- 18.4 MPLS procedures list 18-4**
- 18.5 MPLS procedures 18-5**

18.1 MPLS configuration overview

The 5620 SAM supports the configuration of MPLS paths and LSPs on managed routers, and the provisioning of MPLS paths and LSPs on managed and unmanaged devices.

To configure MPLS-signaled LSPs, you must first create an MPLS path between two routers. An LSP can then be created between the two routers and be bound to an MPLS path. An LSP-MPLS path binding is called an LSP path. You can configure the LSP paths after the MPLS path and the LSP have been associated.

The 5620 SAM supports the configuration of related protocols such as RSVP and LDP on managed routers. MPLS uses RSVP to set up traffic engineered LSPs. LDP performs label distribution in MPLS networks.

MPLS, RSVP, and LDP are enabled on routing instances on routers. When they are enabled, an MPLS, RSVP, or LDP instance is created on the routing instance on the Network tab on the 5620 SAM navigation tree. Various functions can then be performed on the instance. For example, Layer 3 interfaces can be assigned to an MPLS instance.

Services are transported across a network using service tunnels, which can use GRE or MPLS as the underlying transport mechanism. For networks that use MPLS, an MPLS mesh and an LSP mesh should be created before you start associating LSPs with the service tunnels. LSPs and service tunnels are unidirectional, thus both LSPs and service tunnels must be created in both directions.

LSPs can be associated with service tunnels when you configure or modify service tunnels. See chapter 19 for more information about service tunnels.

To configure MPLS paths, choose Topology→MPLS Path Manager from the 5620 SAM main menu. Figure 18-1 shows a Create MPLS Path form.

Figure 18-1 Create MPLS path form - Name the MPLS Path step

The screenshot shows a window titled "Create MPLS Path...". On the left, a "Steps" sidebar lists five steps: "1. Name the MPLS Path..." (highlighted), "2. Define Source Site...", "3. Define Destination Site...", "4. Define the Provisioned Path...", and "5. Set Initial State". The main area is titled "Name the MPLS Path..." and contains the instruction "Provide a name and a description for your new MPLS Path." Below this are two input fields: "Name:" and "Description:". At the bottom, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

To configure LSPs, choose Topology→LSP Manager from the 5620 SAM main menu. Figure 18-2 shows a Create LSP form.

Figure 18-2 Create LSP form - Identification step

The screenshot shows a window titled "LSP Create LSP Wizard -". On the left, a "Steps" sidebar lists five steps: "1. Identification" (highlighted), "2. Define Source Site...", "3. Define Destination Site...", "4. Add LSP Paths...", and "5. Set Initial State". The main area is titled "Identification" and contains the instruction "Provide a name and a description for your new LSP." Below this are three input fields: "Name:" (highlighted in yellow), "Description:", and "ID:" (containing the value "0"). To the right of the "ID:" field is a checked checkbox labeled "Auto-Assign ID". At the bottom, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

See the *7750 SR OS Services Guide* for more information about MPLS, LSPs, RSVP, and LDP.

18.2 Workflow to configure MPLS

- 1 Enable MPLS and LDP on routing instances on all routers that will participate in the MPLS network. RSVP is enabled by default. When MPLS, LDP, or RSVP is enabled on a routing instance, an MPLS, LDP or RSVP instance is created on the routing instance.
- 2 Assign Layer 3 interfaces to MPLS instance and perform additional MPLS interface configurations as required.
- 3 Create a mesh of MPLS paths.
- 4 Create a mesh of LSPs.

18.3 MPLS menus

Table 18-1 lists the Topology menu items that you use to configure MPLS.

Table 18-1 5620 SAM MPLS menus

Menu option	Task
Topology→LSP Manager	Create and configure LSPs and LSP paths
Topology→MPLS Path Manager	Create and configure MPLS paths
Topology→LSP Topology	View the LSP topology map

18.4 MPLS procedures list

Table 18-2 lists the procedures to configure MPLS and related protocols.

Table 18-2 5620 SAM MPLS procedures list

Procedure	Purpose
To enable MPLS on a routing instance	To enable MPLS on a routing instance
To create MPLS interfaces	To assign the MPLS interfaces
To create MPLS paths	To configure MPLS paths
To create LSPs	To configure LSPs
To configure LSP paths	To configure LSP paths
To list MPLS paths	To list MPLS paths

(1 of 2)

Procedure	Purpose
To list LSPs	To view LSPs
To view the LSP topology map	To view the LSP topology map

(2 of 2)

18.5 MPLS procedures

Use the following procedures to configure MPLS.

Procedure 18-1 To enable MPLS on a routing instance

- 1 From the 5620 SAM, select the Network tab on the navigation tree.
 - 2 Navigate to a routing instance.
The navigation path is Network→Router→Routing Instance.
 - 3 Right click on a routing instance and choose Properties from the contextual menu.
The Routing Instance form appears.
 - 4 Click on the Protocols tab.
 - 5 Select the MPLS Enabled and the LDP Enabled check boxes. RSVP-TE is enabled by default and cannot be disabled using the 5620 SAM.
 - 6 Click on the Apply button to save the changes.
An MPLS instance is created for the routing instance in the navigation tree.
-

Procedure 18-2 To create MPLS interfaces

Perform this procedure to create an MPLS interface by assigning a Layer 3 interface to an MPLS instance.

Create and configure Layer 3 interfaces prior to performing this procedure. See section 16.4 for more information about configuring routers and interfaces.

- 1 Select the Network tab on the navigation tree.
- 2 Navigate to the MPLS instance icon.
The navigation path is Network→Router→Routing Instance→MPLS.
- 3 Right-click on the MPLS icon and choose Create Interface from the contextual menu to choose a Layer 3 interface and assign it to the MPLS instance.
The MPLS Interface (Create) form appears.

- 4 Configure the parameters.
 - i Click on the Select button next to the Interface Name parameter to select a Layer 3 interface.

The Select Interface form appears. Select an interface from the list and click on the OK button.

The interface is added to the Interface Name parameter on the MPLS Interface (Create) form.
 - ii Set the Administrative State parameter to Up or Down.
- 5 Click on the Apply button to save the changes.

The MPLS interface is created and added to the MPLS instance on the navigation tree.
- 6 To view the interface configuration and configure some additional parameters, right click on the newly-created interface in the MPLS icon and choose Properties. The MPLS Interface properties form appears with the General tab button selected, as shown in Figure 18-3.

Figure 18-3 MPLS Interface properties form - General

The screenshot displays the 'MPLS Interface - system, 38.120.182.44 [Edit]' window with the 'General' tab selected. The form is organized into several sections:

- Site:** Site ID: 38.120.182.44, Site Name: itb_dave2. Includes a 'View...' button.
- Routing Instance:** Routing Instance ID: 1, Routing Instance Name: Base. Includes 'View...' and 'View MPLS Site...' buttons.
- Interface:** Interface ID: 1, Interface Name: system. Includes a 'View...' button. Other fields: Interface Class: System, Port: n/a, Encapsulation Type: Unknown, Inner Encapsulation Value: 0, Outer Encapsulation Value: 0.
- Protocol:** MPLS, Description: N/A.
- States:** Administrative State: Up (dropdown), Operational State: Unknown, State Qualifier: OK.
- Frame Size Constraints:** Configured Interface/Port MTU (bytes): 1500, Operational Interface/Port MTU (bytes): 1500.

At the bottom, there are control buttons: Turn Up, Shut Down, View RSVP Interface..., Delete..., Resync, Reset, OK, Cancel, and Apply.

The MPLS Interface properties form contains the tabs described in Table 18-3.

Table 18-3 MPLS Interface properties form

Tab	Description
General	View general interface configuration information, and configure the following parameters. <ul style="list-style-type: none"> • Protocol Description • Administrative State. The options are Up or Down.
Administrative Groups	Assign or unassign MPLS administrative groups to the interface. After you assign administrative groups to an MPLS interface, the total value of the groups is displayed in 32 bit mask format in the Administrative Groups: Groups Included parameter of the General tab.
In Labels	View in label information
Crossconnects	View crossconnect information
Out Labels	View out label information
Statistics	View statistical information
Faults	View alarm information

- 7 Click on the Apply button to save changes, if required.
- 8 Click on the OK button to close the form.

Procedure 18-3 To create MPLS paths

- 1 Select Topology→MPLS Path Manager from the 5620 SAM main menu.
The MPLS Path Manager filter form appears.
- 2 Click on the Create MPLS Path button.
The Create MPLS path form appears, as show in Figure 18-4. Configure the parameters, and click on the Next button to proceed to the next step in the configuration.

Figure 18-4 Create MPLS Path form - Name the MPLS Path step

The screenshot shows a web-based form titled "Create MPLS Path...". On the left, a "Steps" sidebar lists five steps: "1. Name the MPLS Path...", "2. Define Source Site...", "3. Define Destination Site...", "4. Define the Provisioned Path...", and "5. Set Initial State". Step 1 is highlighted in blue. The main content area is titled "Name the MPLS Path..." and includes the instruction "Provide a name and a description for your new MPLS Path." Below this instruction are two text input fields: "Name:" and "Description:". At the bottom of the form, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

3 Name the MPLS path and provide a description, if required.

Click on the Next button.

4 Define the source site. Specify a managed device by entering an IP address. You can also specify a managed device by clicking on the Select button and selecting a device from the list.

Click on the Next button.

5 Define the destination site.

- Specify a managed or unmanaged device by clicking on the Specify Site: Manually button, and specifying an IP address.
- You can also specify a managed router by clicking on the Specify Site: By Selection button, clicking on the Select button next to the Network Element parameter, and choosing a managed device from the list.
To specify a Layer 3 interface as the destination, first specify a device, and then click on the IP Address parameter Select button and select an interface. You can also manually enter an IP address for the interface.
- Specify whether you want the last hop type to be strict or loose.
When you choose strict, LSPs must take a direct path from the previous hop device to the destination device. When you choose loose, the LSP can traverse other devices.

Click on the Next button.

6 Define the provisioned path by inserting hops.

- i Click on the Insert Hop button.

The Hop for New Tunnel form appears.

- ii Specify a managed or unmanaged device by clicking on the Specify Site: Manually button, and specifying an IP address.

You can also specify a managed router by clicking on the Specify Site: By Selection button by clicking on the Select button, and choosing a managed device.

- iii Specify whether you want the hop type to be strict or loose.
- iv Click on the Apply button to save the configuration or click on the OK button to save the configuration and close the insert hop form. When you close the form, the hops appear in a list in the MPLS path configuration form.

To add additional hops, click on the Insert Hop button. To change the hop sequence, choose a hop and click the Move Up or Move Down button

- v Select the hops from the list.

Click on the Next button.

- 7 Set the administrative state of the MPLS path to Up or Down.
- 8 Click on the Finish Button to save the configuration.
The 5620 SAM prompts you to view the MPLS path.
- 9 Select the check box to view the MPLS path configuration.

Procedure 18-4 To create LSPs

Create and configure a mesh of MPLS paths prior to performing this procedure.

- 1 Choose Topology→LSP Manager from the 5620 SAM main menu.
The LSP Manager form appears.
- 2 Click on the Create LSP button. The Create LSP form appears with the Identification parameters displayed as shown in Figure 18-5.

Figure 18-5 Create LSP form - Identification step

The screenshot shows a software window titled "LSP Create LSP Wizard -". On the left, a "Steps" pane lists five steps: "1. Identification" (highlighted), "2. Define Source Site...", "3. Define Destination Site...", "4. Add LSP Paths...", and "5. Set Initial State". The main area, titled "Identification", contains three input fields: "Name:" (with a yellow highlight), "Description:", and "ID:" (containing the value "0"). A checkbox labeled "Auto-Assign ID" is checked. At the bottom right, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Configure the parameters.

- i Enter a name for the LSP.
- ii Enter a description for the LSP.
- iii Specify how you want to assign LSP IDs.
 - To have policy IDs automatically assigned, select the Auto-Assign ID check box.
 - To manually assign a policy ID, deselect the Auto-Assign ID check box and enter an ID.
- 3 Click on the Next button. The Define Source Site form appears. Configure the parameters.
 - i Click on the Source Site ID parameter Select button and choose a source device from the list. You can also manually specify an IP address.
 - ii If required, click on the Source Site IP Address parameter Select button and choose a source interface. You can also manually specify an IP address.
- 4 Click on the Next button. The Define Destination Site step appears. Configure the parameter.

Click on the Destination Site ID parameter Select button and choose a destination device from the list. You can also manually specify an IP address. The LSP must terminate on the system interface, whose IP address is the same IP address as that of the device.

- 5 Click on the Next button. The Add LSP Paths step appears.
 - i Set the Tunnel Destination Matching parameter to Destination Site or None.
 - ii Click on the Add button. The LSP path association step appears with the Choose LSP Path Type parameters displayed.
 - iii Choose an LSP path type. An LSP path is an LSP which is associated with an MPLS path. The options are primary, secondary, or standby.
 - iv Click on the Next button. The Choose MPLS Path step appears with a list of available MPLS paths. Choose an MPLS path to associate with the LSP.
 - v Click on the Next button. The Set Traffic Options step appears. Configure the parameters.
 - Specify a value for the Reserved Bandwidth parameter. The parameter specifies the minimum amount of the bandwidth of the MPLS path to be reserved for the LSP. The range is 0 to 100 000.
 - Select the Inherit Value check box if you want the LSP path to inherit the Hop Limit parameter from the associated LSP. Deselect the Inherit Value check box if you want to specify a hop limit for the LSP path.
 - If you deselected the Inherit Value check box, specify a value for the Hop Limit parameter. The range is 2 to 255.
 - Set the Record Actual Path parameter to True or False. The parameter specifies whether the actual path will be recorded and shown for the LSP Path. The options are True or False.
 - vi Click on the Next button. The Set Initial States step appears. Set the initial state to Up or Down
 - vii Click on the Finish button.

The LSP path association form closes and the LSP path appears in the LSP path list in the Create LSP form. To configure additional LSP path parameters, choose the LSP path and click the Edit button. See Procedure 18-5 for more information about configuring LSP path parameters.
 - viii Choose an LSP path from the list.
- 6 Click on the Next button. Set the administrative state of the LSP to Up or Down.
- 7 Click on the Finish Button to save the configuration.
- 8 The 5620 SAM prompts you to view the LSP. Select the check box and click on the Close button in the Create LSP form to view the LSP properties form with the General tab button selected, as shown in Figure 18-6.

Figure 18-6 LSP properties form - General

The screenshot shows a software interface for configuring an LSP. The title bar reads "DynamicLsp - lsp_44-18; id 1, from itb_dave2 (38.120.182.44) to pc18 (10.1.1.18) [Edit]". Below the title bar are several tabs: "Services", "Service Tunnels", "Circuits", "Subscribers", "Administrative Groups", "Statistics", and "Faults". The "General" tab is selected and contains the following sections:

- Identity:** Name: ; Description: ; ID: ; Type: ; Maximum Transmitted Frame Size (MTU) (bytes): ; Preference:
- Source:** Source Site ID: ; Source Site Name: ; Source IP Address: ; Source Interface Name: ; Ingress Interface ID: ; Ingress Interface Name: ; Ingress Label: . There are "Select..." and "View..." buttons for the Source Interface Name and Ingress Interface Name fields.
- Destination:** Destination Site ID: ; Destination Site Name: ; Destination IP Address: ; Destination Interface Name: ; Egress Interface ID: ; Egress Interface Name: ; Egress Label: . There are "View..." buttons for the Destination Interface Name and Egress Interface Name fields.
- States:** Administrative: ; Operational:

At the bottom of the form are several action buttons: "Resync", "Remove", "Turn Up", "Shut Down", "Reset", "OK", "Cancel", and "Apply".

The LSP properties form contains the tabs described in Table 18-4.

Table 18-4 LSP properties form

Tab	Description
General	View general LSP configuration information, and configure the following parameters. <ul style="list-style-type: none"> Description LSP Preference. The range is 1 to 255. Source Interface Administrative State. The options are Up or Down.
Properties	View LSP properties and configure the following parameters. <ul style="list-style-type: none"> Fast Reroute. The options are true or false. Hop Limit. The range is 2 to 255. When you specify True for Fast Reroute, the following parameters appears. <ul style="list-style-type: none"> Fast Reroute: Backup Type. The options are One to One or Many to One. Fast Reroute: Hop Limit. The range is 0 to 255. Fast Reroute: Reserved Bandwidth (Mbps). The range is 0 to 10 000. Fast Reroute: Node Protect. The options are True or False. Make Before Break. The parameter specifies whether make before break will be performed for the primary and secondary LSP paths. The options are True or False. CSPF: Enable CSPF. The options are true or false. CSPF: Optimize Timer. The parameter specifies that CSPF will recalculate the LSP path after the timer expires. If a new path is found, the LSP is signaled on the new path. If make-before-break is enabled, the transition to the new path does not cause any traffic disruption. The range is 0 to 65 535. Retry Timer (seconds). The range is 1 to 600. Retry Limit. The range is 0 to 10 000. RSVP Reserve Style. The options are Shared-Explicit or Fixed Filter. Include ADSPEC in RSVP. The options are True or False.
LSP paths	View and manage LSP paths
CrossConnects	View and manage crossconnects
RSVP Sessions	View and manage RSVP sessions
Services	View and manage services
Service Tunnels	View and manage service tunnels
Circuits	View and manage circuits
Subscribers	View and manage subscribers
Administrative Groups	Assign MPLS administrative groups to be included or excluded for the LSP, and you can unassign MPLS administrative groups. After you assign administrative groups to an LSP, the total value of the groups is displayed in 32 bit mask format and the Administrative Groups: Groups Included and the Administrative Groups: Groups Excluded parameters of the General tab.
Maintenance	View and perform OAM diagnostics. See chapter 29 for more information.
Statistics	View and manage statistical information
Faults	View and manage alarms

Procedure 18-5 To configure LSP paths

An LSP path is an LSP-MPLS path binding.

- 1 Choose Topology→LSP Manager from the 5620 SAM main menu. The LSP Path Manager form appears.
- 2 Configure the search filter parameters and click on the Search button. A list of LSPs is displayed.
- 3 From the General tab, choose an LSP and click the on Edit button. The LSP properties form appears.
- 4 Choose the LSP Paths tab. A list of LSP paths is displayed.
- 5 Choose an LSP path and click on the Edit button. The LSP paths properties form appears with the General tab button selected, as shown in Figure 18-7.

Figure 18-7 LSP path properties form - General

The screenshot shows the 'LSP Path - mplspath_44-18; id 1; Lsp lsp_44-18; id 5 (from itb_dave2 (38.120.182.44) to pc18 (10.1.1.18) [Edit]' window. The 'General' tab is selected. The form contains the following fields and sections:

- General Information:** LSP Name: lsp_44-18, LSP ID: 5, MPLS Path Name: mplspath_44-18, MPLS Path ID: 1, Type: primary, Status: inactive.
- States:** Administrative: Up, Operational: Down, Fail Code: Routing Error, Failed Site ID: 38.120.182.44.
- Transport Properties:** Maximum Transmitted Frame Size (MTU): 0.
- Traffic Engineering Properties:** Reserved Bandwidth (Mbps): 0, Hop Limit: 255, Record Actual Path: true, Inherit Value (checked).
- Make before Break:** Make before Break: true, Operational Bandwidth (Mbps): 0, State: none, Resignat: N/A, Inherit Value (checked).
- CSPF:** Optimize Timer (seconds): 0, Next Optimization (seconds): 0, Inherit Value (checked).
- Buttons:** Enable OAM, Disable OAM, View MPLS Path..., Turn Up, Shut Down, Delete, Resync, Reset, OK, Cancel, Apply.

The LSP Path properties form contains the tabs described in Table 18-5.

Table 18-5 LSP path properties form

Tab	Description
General	<p>View general LSP path configuration information, and configure the following parameters.</p> <ul style="list-style-type: none"> • Administrative State. The options are Up or Down. • Reserved Bandwidth (Mbps). The range is 0 to 100 000. • Hop Limit: Inherit Value. Select the check box for the LSP path to inherit the Hop Limit parameter from the LSP. • Hop Limit. If you deselected the Inherit Value check box, configure the Hop Limit parameter for the LSP path. The range is 2 to 255. • Make Before Break: Inherit Value. Select the check box for the LSP path to inherit the Make Before Break parameter from the LSP. • Make Before Break. If you deselected the Make Before Break: Inherit Value check box, configure the Make Before Break parameter. The parameter specifies whether before break will be performed for the primary path and all the secondary LSP paths. The options are True or False. • Make Before Break: Resignal. The options are N/A or Do Action. • CSPF: Inherit Value. Select the check box if you want the LSP path to inherit the Optimize Timer parameter from the associated LSP. CSPF is automatically enabled on LSP paths when it is enabled on the LSP. • Optimize Timer. If you deselected the CSPF: Inherit Value check box, configure the Optimize Timer parameter. CSPF will recalculate the LSP path when the timer expires. If a new path is found, the LSP is resigaled on the new path. If make before break is enabled, transition to the new path will not cause traffic disruption. The range is 0 to 65 535. • Administrative Group: Groups Included. Select the check box if you want the LSP path to inherit included administrative groups from the LSP. • Administrative Group: Groups Excluded. Select the check box if you want the LSP path to inherit excluded administrative groups from the LSP.
Maintenance	<p>View maintenance properties and enable OAM using the check box. Click on the Apply button.</p> <p>When OAM is enabled, you can run LSP ping and trace OAM tests. See chapter 29 for more information.</p>
Provisioned Path	View the provisioned LSP path
Actual Path	View the actual path
CPSF Path	View the CPSF path
Administrative Groups	<p>Assign MPLS administrative groups to be included or excluded for the LSP path, and you can unassign MPLS administrative groups.</p> <p>After you assign administrative groups to an LSP path, the total value of the groups is displayed in 32 bit mask format and the Administrative Groups: Groups Included and the Administrative Groups: Groups Excluded parameters of the General tab.</p>
Faults	View and manage alarms

Procedure 18-6 To list MPLS paths

- 1 Choose Topology→MPLS Path Manager from the 5620 SAM main menu.
The MPLS Path Manager form appears.
- 2 Configure the search filter parameters.

- 3 Click on the Search button.
A list of MPLS paths is displayed.
-

Procedure 18-7 To list LSPs

- 1 Choose Topology→LSP Manager from the 5620 SAM main menu.
The LSP Manager form appears.
 - 2 Configure the search filter parameters.
 - 3 Click on the Search button.
A list of LSPs is displayed.
-

Procedure 18-8 To view the LSP topology map

- 1 Choose Topology→LSP Topology from the 5620 SAM main menu.
The LSP Network Element Filter form appears.
 - 2 Configure the filter parameters.
 - 3 Click on the OK button.
The LSP topology map appears.
-

19 — Service tunnels

- 19.1 Service tunnel overview 19-2**
- 19.2 Service tunnel menus 19-3**
- 19.3 Service tunnel procedure list 19-3**
- 19.4 Configuring service tunnels procedures 19-4**

19.1 Service tunnel overview

Distributed VLL service and VPLS traffic is transported between edge-managed routers by circuits aggregated in unidirectional service tunnels. Service tunnels originate on a source router and terminate on a destination router, which directs packets to the correct service egress access interface.

The operational theory of a service tunnel is that the encapsulation of the data between the two managed edge routers appears like a Layer 2 path to the service data although it is really traversing an IP or IP/MPLS core.

Service tunnels are not used for local VLL service or VPLS because the same router is the source and destination router.

Service tunnels can be configured to use GRE or MPLS. In the case of MPLS, a mesh of MPLS paths and LSPs must first be created in the network core. Service tunnels can then be associated with LSPs during service tunnel configuration or modification.

Tunnel configuration for a VLL service or VPLS should be performed before you configure the service. The tunnel, which is identified on a router by a unique ID, is bound to a service when you configure the service.

The 5620 SAM supports service tunnel configuration using a sequence of configuration forms and steps. To create a service tunnel, choose Topology→Service Tunnel Manager from the 5620 SAM main menu and click on the Create Service Tunnel (SDP) button. Figure 19-1 shows the initial Create Service Tunnel (SDP) form with the Name & Describe Service Tunnel (SDP) parameters displayed.

Figure 19-1 Create Service Tunnel (SDP) form - Name & Describe Service Tunnel (SDP) form

When you configure a service tunnel, consider the following:

- Service tunnels must be created in both directions: from the source edge router to a destination edge router, and from the destination edge router back to the source edge router.
- The tunnel is not specific to any one service or any type of service. Once a tunnel is created, multiple service circuits can be aggregated over the tunnel. The aggregated circuits can belong to different services and different subscribers.
- All services that are mapped to a tunnel use the same transport encapsulation type defined for the tunnel (either GRE or MPLS).
- Operations on the tunnel affect all the services that are associated with the tunnel. For example, the operational and administrative state of a tunnel controls 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 or circuit carried by the tunnel.
- The tunnel is locally unique to a participating router. The same tunnel ID can appear on other routers.
- A tunnel uses the system IP address to identify the far-end edge router.

See the *7750 SR OS Services Guide* for more detailed information about service tunnels.

19.2 Service tunnel menus

Table 19-1 lists and describes the 5620 SAM service tunnel menus.

Table 19-1 Service tunnel menus

Menu item	Description
Topology→Service Path Topology	View a map of the service tunnels that are managed by the 5620 SAM
Topology→Service Tunnel Manager	Create and manage service tunnels

19.3 Service tunnel procedure list

Table 19-2 lists the procedure necessary to perform service tunnel tasks.

Table 19-2 Service tunnel procedure list

Procedure	Purpose
To configure service tunnels	Create a service tunnel
To list service tunnels	List service tunnels
To view the service tunnel topology map	View a map of the service tunnels that are managed by the 5620 SAM

19.4 Configuring service tunnels procedures

Procedure 19-1 describes how to configure service tunnels.

Procedure 19-1 To configure service tunnels

- 1 Choose Topology→Service Tunnel Manager from the 5620 SAM main menu.

The Service Tunnel Manager form appears.

- 2 Click on the Create Service Tunnel (SDP) button.

The Create Service Tunnel (SDP) form appears with the Name & Describe Service Tunnel (SD) parameters displayed, as shown in Figure 19-2.

Figure 19-2 Create Service Tunnel (SDP) form - Name & Describe Service Tunnel (SDP) form

The screenshot shows a software window titled "Create Service Tunnel (SDP)...". On the left, a "Steps" sidebar lists seven steps, with the first step, "1. Name & Describe Service Tunnel (SDP)", highlighted in cyan. The main area of the window is titled "Name & Describe Service Tunnel (SDP)" and contains the following form elements:

- "Name:" followed by a text input field.
- "Description:" followed by a text input field.
- "ID:" followed by a text input field containing the number "0".
- A checkbox labeled "Auto-Assign ID" which is checked.

At the bottom of the window, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

A series of steps and parameters appear. Configure the parameters, and click on the Next button to go to the next step.

- i** Name and describe the service tunnel. Configure the following parameters:
 - Name to name the service tunnel
 - Description of the service tunnel
 - ID. Click on the Auto-Assign ID check box if you want the 5620 SAM to automatically assign IDs.
- ii** Pick Source Node. Specify a source node by entering the IP address for the Source Site ID parameter. Alternately, you can click on the Select button and choose a source node from the Select Network Element list.
- iii** Pick Destination Node. Specify a destination by entering the IP address for the Destination Site ID parameter. Alternately, you can click on the Select button and choose a destination node from the Select Network Element list.
- iv** Specify Transport. Configure the following parameters:
 - Underlying Transport. The options are GRE or MPLS.
 - Signalling. When you choose MPLS as the for the Underlying Transport parameter, the options for the signalling parameter are TLDP or None (manual). When you choose GRE for the Underlying Transport, the Signalling parameter is not available.
- v** Associate LSPs (only appears if you chose MPLS as the underlying transport protocol.) Click on the Add button and follow the steps to bind LSPs to the service tunnel.
- vi** Specify AutoSelection Parameters. Configure the following parameters:
 - AutoSelection Enabled. Click on the check box to enable or disable autoselection.
 - Selectable for Forwarding Classes. Click on the one or more of the check boxes. The options are be, af, h2, h1, l2, l1, ef, nc.
You should carefully plan your forwarding classes for the service tunnels, so that they map to the QoS parameters configured for subscriber services, such as VLL. See the *7750 SR OS Services Guide* for more information.
 - Autoselection Preference. Specify a numerical value.
- vii** Specify Hello Parameters. Configure the following parameters:
 - Keep-alive Enabled. Select the check box to enable or disable keep-alive.
 - Hello Time. Specify a numerical value from 1 to 3600.
 - Hello Request Timeout. Specify a numerical value from 1 to 10.
 - Mac Drop Count. Specify a numerical value from 1 to 5.
 - Hello Message Length. Specify 0 or a numerical value from 40 to 9198.
 - Hold Down Time. Specify a numerical value from 1 to 3600.
- viii** Specify Initial State. Configure the following parameters:
 - Administrative State. The options are Up or Down.
 - Administrative MTU. Specify a numerical value from 0 to 9194.

- 3 Click on the Finish button to save the configuration.

The 5620 SAM prompts you to view the service tunnel configuration.

- 4 Select the check box to view the service tunnel configuration.

- 5 Click on the Close button.

The 5620 SAM displays the service tunnel configuration.

To view the service tunnel map, choose Topology→Service Path Topology from the 5620 SAM main menu.

Procedure 19-2 To list service tunnels

- 1 Choose Topology→Service Tunnel Manager from the 5620 SAM main menu.

The Service Tunnel Manager form appears.

- 2 Configure the list filter parameters.

- 3 Click on the Search button.

A list of service tunnels appears.

Procedure 19-3 To view the service tunnel topology map

- 1 Choose Topology→Service Path Topology from the 5620 SAM main menu.

The Service Path Topology form appears. A service tunnel is also called a service path.

- 2 Configure the map filter parameters.

- 3 Click on the OK button.

The service tunnel topology map appears. See section 27.1 for more information about the service tunnel topology map.

Managing subscriber services

- 20 — Policies**
- 21 — Subscriber configuration and management**
- 22 — Service management overview**
- 23 — VLL service management**
- 24 — VPLS management**
- 25 — IES management**
- 26 — VPRN service management**
- 27 — Map management**

20 — Policies

- 20.1 Policies overview 20-2**
- 20.2 Service management policies 20-5**
- 20.3 Workflow to create policies 20-17**
- 20.4 Policies menu 20-17**
- 20.5 Policies procedures list 20-18**
- 20.6 Policies procedures 20-19**

20.1 Policies overview

The 5620 SAM supports the template-based creation of rules. These rules are called policies. There are three types of policies:

- service management policies
- routing management policies
- network management policies

Service management policies specify how service traffic is handled by network resources such as interfaces, ports, daughter cards, and circuits. These policies can be used by multiple resources on multiple services. Examples of service management policies include access ingress, access egress, and network policies.

Routing management policies specify routing configuration according to specifically defined parameters. There are two routing management policies; routing policies and MPLS administrative group policies.

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 used for billing, and stores information. Examples of network management policies include alarm, mediation, and accounting policies.

Table 20-1 describes the policies that can be configured using the 5620 SAM. Unless otherwise noted in the table, the policies are described in more detail in this chapter.

Table 20-1 Policies

Policy type	Policy	Applied to	Description	Menu option
Service management	Access Ingress	Access interface	Defines ingress classification, policing, shaping, and marking on the ingress side of the interface.	Policies→Access Ingress Policy Manager
	Access Egress	Access interface	Defines egress classification, policing, shaping, and marking on the egress side of the interface.	Policies→Access Egress Policy Manager
	Network Policy	Network interface	Defines egress QoS marking and ingress QoS interpretation for traffic on core network IP interfaces.	Policies→Network Policy Manager
	Slope	Access port Network daughter card Network port	Defines RED slope behavior.	Policies→Slope Policy Manager
	Network Queue	Network daughter card Network port	Defines the default buffer allocations for queues based on the queue's forwarding class.	Policies→Network Queue Policy Manager
	Scheduler	Access ingress interface Access egress interface	Defines hierarchical rate limiting and scheduling to govern queue scheduling.	Policies→Scheduler Policy Manager
	ACL IP Filter	Network interface Access interface Circuit	Controls network traffic into or out of an interface or circuit based on IP matching criteria.	Policies→Acl IP Filter Manager
	MAC IP Filter	Access interface Circuit	Controls network traffic into or out of an interface or circuit based on MAC matching criteria.	Policies→Acl MAC Filter Manager
Routing management	Routing	Routing instance	Manages route policies. See chapter 16 for more information.	Policies→Routing Policy Manager
	Admin Group (MPLS) policy manager	MPLS interfaces LSPs LSP paths	Configures MPLS administrative groups and defines the groups to which an MPLS interface, LSP, or LSP path belongs. See chapter 16 for more information.	Policies→Admin Group (MPLS) Policy Manager
Network management	Alarm	Alarm logs Alarms	Defines how the 5620 SAM handles individual incoming alarms, and how alarm logs are created and stored. See chapter 28 for more information.	Policies→Alarm Policies
	File	—	Manages files on the device. See chapter 30 for more information.	Policies→File Policy Manager
	Accounting	Network interface Access interface Circuit	Manages accounting policies. See chapter 30 for more information.	Policies→Accounting Policy Manager
	Mediation	5620 SAM	Defines how the 5620 SAM communicates with the network. See chapter 10 for more information.	Mediation→Deployment and Site Backup/Upgrade
	Poller	5620 SAM	Defines how the 5620 SAM polls the network. See chapter 6 for more information.	Mediation→Poller Policies

The 5620 SAM supports the creation and modification of policies using configuration forms. For example, Figure 20-1 shows an Access Ingress Policy form with the General tab button selected.

Figure 20-1 Access Ingress Policy form - General

The screenshot shows a web-based configuration form for an Access Ingress Policy. The window title is "Policy, Access Ingress:0 [Create]". The form has several tabs: "MAC Match Criteria", "Definitions", "Access L2 Interfaces", "L3 Interfaces", "Relations", "General", "Queues", "Forwarding Classes", "Dot1p", "Dscp", "Precedence", and "IP Match Criteria". The "General" tab is selected. The form contains the following fields and controls:

- Configuration Action:** A dropdown menu set to "Merge With Existing".
- ID:** A text input field containing "0" and a checked checkbox labeled "Auto-Assign ID".
- Displayed Name:** An empty text input field.
- Description:** An empty text input field.
- Properties:** A section containing:
 - Default FC:** A dropdown menu set to "be".
 - Priority:** A dropdown menu set to "low".

At the bottom of the form are four buttons: "Reset", "OK", "Cancel", and "Apply".

Policies are applied to resources during service configuration or modification. Policies are also applied to resources before or after the service is configured by choosing and modifying the resource from the equipment manager, subscriber manager, or service manager forms. Figure 20-2 shows the Create L2 Interface form that appears during VLL service creation with the Select Site parameters displayed. Note the steps to specify policies for the interface.

Figure 20-2 Create L2 Interface form - Select Site form

Steps

1. Select Site
2. Select Port
3. Define General Properties
4. Select QoS Policies
5. Aggregation
6. Select Ingress and Egress Scheduler Policies
7. Select ACL Filters
8. Select Accounting Policy

Select Site

Sites In This Service:

Site ID	Site Name	
10.1.1.30	pc30	1500
10.1.1.31	pc31	1500

Buttons: Edit..., Select Other...

Site ID: Site Name:

Buttons: < Back, Next >, Finish, Cancel

20.2 Service management policies

This section describes the service management policies.

Access ingress policies

Access ingress policies are applied to access interfaces and specify QoS on ingress. Figure 20-3 shows an Access Ingress Policy form with the General tab button selected.

Figure 20-3 Access Ingress Policy form - General

Policy, Access Ingress:0 [Create]

MAC Match Criteria Definitions Access L2 Interfaces L3 Interfaces Relations

General Queues Forwarding Classes Dot1p Dscp Precedence IP Match Criteria

Configuration Action

Configuration Action: Merge With Existing ▼

ID: 0 Auto-Assign ID

Displayed Name:

Description:

Properties

Default FC: be ▼ Priority: low ▼

Reset OK Cancel Apply

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 will not be 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
- 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
- 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

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.

See the *7750 SR OS Services Guide* for more detailed information about access ingress policies.



Note — The 5620 SAM supports the configuration of HQoS scheduling mechanisms on the 7750 SR. HQoS provides the ability to rate limit across multiple queues from either single or multiple access interfaces for a given customer. The building blocks for HQoS include access ingress, access egress, and scheduler policies.

See chapter 22.3 for a sample service configuration using HQoS.

Forwarding classes

The 5620 SAM supports the configuration of eight forwarding classes and class-based queuing on the 7750 SR. Each forwarding class is only important in relation to other forwarding classes. A forwarding class provides network elements 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. Eight forwarding classes are supported. Table 20-2 lists the default definitions for the supported forwarding classes.

Table 20-2 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			

Access egress policies

Access egress policies are applied to access egress interfaces and specify QoS on egress. Figure 20-4 shows an Access Egress Policy form with the General tab button selected.

Figure 20-4 Access Egress Policy form - General

The screenshot shows a web-based configuration form for an Access Egress Policy. The title bar indicates the policy name is 'Policy, Access Egress:0' and it is in 'Create' mode. The 'General' tab is active, showing the following fields:

- Configuration Action:** A dropdown menu currently set to 'Merge With Existing'.
- ID:** A text input field containing the value '0'. To its right is a checked checkbox labeled 'Auto-Assign ID'.
- Displayed Name:** An empty text input field.
- Description:** An empty text input field.

At the bottom of the form, there are four buttons: 'Reset', 'OK', 'Cancel', and 'Apply'.

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.

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.

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 in the 7750 SR 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 ingressed the service on the same 7750 SR, 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 ingress policy. The default policy gives all traffic equal priority with the same chance of being sent or dropped during periods of congestion.

See the *7750 SR OS Services Guide* for more detailed information about access egress policies.

Network policies

Network policies are applied to network interfaces and specify QoS on egress and ingress. Figure 20-5 shows a Network Policy form with the General tab button selected.

Figure 20-5 Network Policy form - General

Policy, Network:0 [Create]

Ingress DSCP Ingress Dot1p Definitions L3 Interfaces

General Egress Forwarding Classes Ingress LSP EXP Bits

Configuration Action

Configuration Action: Merge With Existing ▼

ID: 0 Auto-Assign ID

Displayed Name:

Description:

Ingress

Default FC: l2 ▼ Default FC Profile: in ▼

Egress

Remark: false ▼

Reset OK Cancel Apply

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.

See the *7750 SR OS Services Guide* for more detailed information about network policies.

Network Queue policies

Network Queue policies are applied to network ports or daughter cards. Figure 20-6 shows the Network Queue Policy form with the General tab button selected.

Figure 20-6 Network Queue Policy form - General

The screenshot shows a software window titled "Policy, Global Policy- [Create]". It has several tabs: "General", "Queues", "Forwarding Classes", "Definitions", "Ports", and "MDAs". The "General" tab is selected. The main area contains a "Configuration Action" dropdown menu with "Merge With Existing" selected. Below this are two text input fields: "Displayed Name" (highlighted in yellow) and "Description". At the bottom right, there are four buttons: "Reset", "OK", "Cancel", and "Apply".

Network queue policies determine:

- the default buffer allocations for queues based on the queue's forwarding class
- the CIR, PIR, and burst size parameters for the queue

For network egress, a network buffer policy is associated with the network port buffer pool. For network ingress, the network buffer policy is associated the network ingress buffer pool of the daughter card.

See the *7750 SR OS Services Guide* for more information about network queue policies.

Slope policies

Slope policies are applied to access ports, network ports, and network daughter cards. Figure 20-7 shows a Slope Policy form with the General tab button selected.

Figure 20-7 Slope Policy form - General

Policy, Global Policy - [Create]

General Slopes Definitions

Configuration Action: Merge With Existing

Displayed Name: [Yellow Highlighted Field]

Description: [Empty Field]

Time Average Factor (weight): 7

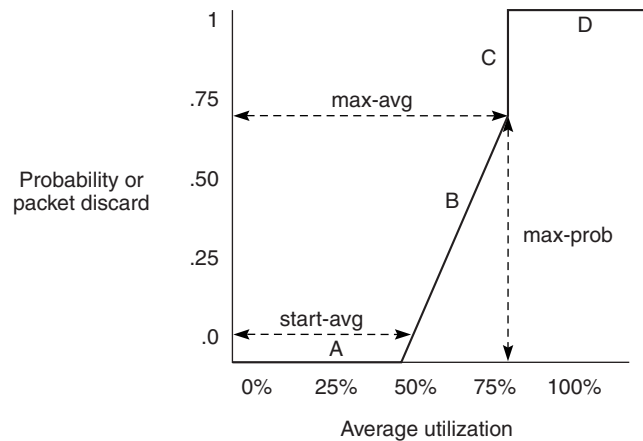
Reset OK Cancel Apply

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 can be defined as four sections, as shown in Figure 20-8.

Figure 20-8 RED slope characteristics



17177

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 a linear slope 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.

See the *7750 SR OS Services Guide* for more detailed information about slope 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:

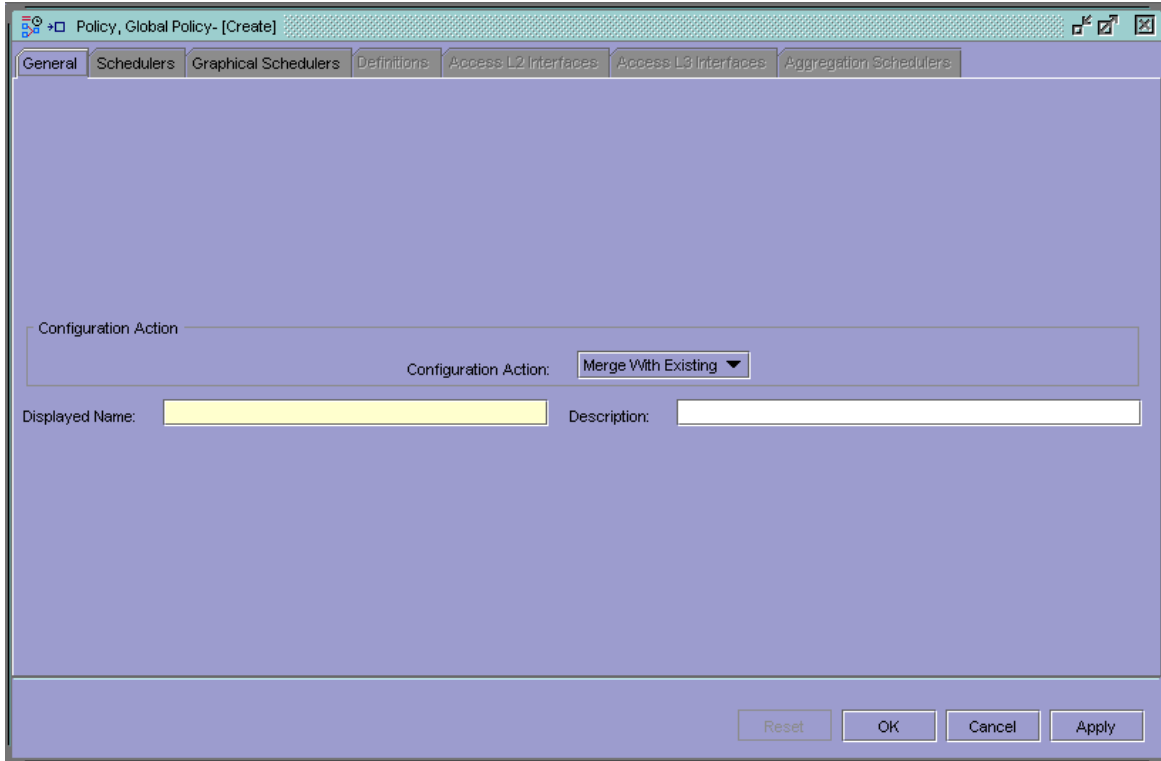
- service ingress queues to switch fabric destinations
- service egress queues to access egress ports
- network ingress queues to switch fabric destinations
- network egress queues to network egress interfaces

The scheduler policies are:

- 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. Figure 20-9 shows a Scheduler Policy form with the General tab button selected.

Figure 20-9 Scheduler Policy form - General



The screenshot shows a web-based configuration interface for a Scheduler Policy. The window title is "Policy, Global Policy- [Create]". The interface has a tabbed menu at the top with the following tabs: "General" (selected), "Schedulers", "Graphical Schedulers", "Definitions", "Access L2 Interfaces", "Access L3 Interfaces", and "Aggregation Schedulers". The main content area is a light purple color. In the lower section, there is a "Configuration Action" field with a dropdown menu currently set to "Merge With Existing". Below this, there are two input fields: "Displayed Name:" (highlighted in yellow) and "Description:". At the bottom right of the form, there are four buttons: "Reset", "OK", "Cancel", and "Apply".

Single tier schedulers

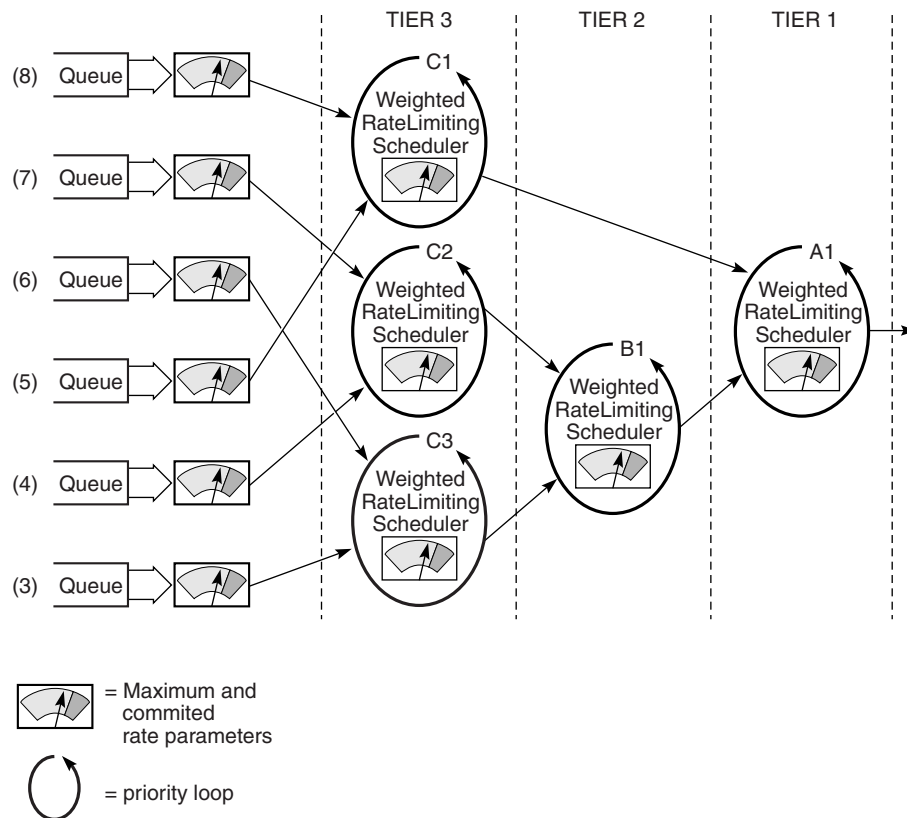
Single tier scheduling is the default method of scheduling queues. Queues are scheduled with single-tier scheduler policies when no explicit hierarchical scheduler policy is defined or applied. In single-tier scheduling, queues are scheduled based on the forwarding class of the queue and the operational state of the queue relative to the queue CIR and PIR.

Hierarchical schedulers

Hierarchical scheduler policies can be 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 can be 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 20-10. 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.

Figure 20-10 Hierarchical scheduler and queue association



17176

Filter policies

IP and MAC filter policies, which are also called ACLs, specify a forward or drop action for packets based on information specified in the match criteria. You can create up to 2000 IP and 2000 MAC filter policies per node. You can create up to 65 535 entries in each 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 on the ingress and egress interfaces. By default, there are no filters associated with services or interfaces.

There are two types of filter policies:

- Acl IP filter policies
- Acl MAC filter policies

Acl IP filters are applied to network IP interfaces, access interfaces, and circuits. Figure 20-11 shows an Acl IP Filter Policy form with the General tab button selected.

Figure 20-11 Acl IP Filter Policy form - General

The screenshot shows a window titled "IpFilter, [Create]" with a menu bar containing "Access L3 Interfaces", "Network L3 Interfaces", "Circuits", and "Definitions". Below the menu bar are three tabs: "General" (selected), "Filter Entries", and "Access L2 Interfaces". The main area contains the following fields:

- Configuration Action: Merge With Existing (dropdown)
- Filter ID: 0 (text box) with a checked "Auto-Assign ID" checkbox
- Displayed Name: (empty text box)
- Description: (empty text box)
- Policy Type: IP Filter (dropdown)
- Is Local: (unchecked checkbox)
- Default Action: forward (dropdown)

At the bottom right, there are four buttons: "Reset", "OK", "Cancel", and "Apply".

Acl MAC filters are applied to access interfaces and circuits. Figure 20-12 shows an Acl MAC Filter Policy form with the General tab button selected.

Figure 20-12 Acl MAC Filter Policy form - General

MacFilter, [Create]

General Filter Entries Access L2 Interfaces Circuits Definitions

Configuration Action: Merge With Existing ▼

Filter ID: 0 Auto-Assign ID

Displayed Name:

Description:

Policy Type: MAC Filter

Is Local:

Default Action: forward ▼

Reset OK Cancel Apply

See the *7750 SR OS Router Guide* for more detailed information about filter policies.

20.3 Workflow to create policies

- 1 Create policies as required.
- 2 Distribute policies. Note that policies do not have to be explicitly distributed — they are distributed to a device when assigned to a resource on the device.
- 3 Assign policies to resources during service configuration or modification.

20.4 Policies menu

Table 20-3 lists and describes the 5620 SAM policies menu options.

For information about alarm policies, see chapter 28. For information about file and accounting policies, see chapter 30. For information about mediation policies, see chapter 10.

Table 20-3 Policies menu

Menu item	Description
Policies→Access Ingress Policy Manager	Create service ingress QoS policies to map ingress traffic to forwarding class queues.
Policies→Access Egress Policy Manager	Create service egress QoS policies to map forwarding classes to service egress queues.
Policies→Network Policy Manager	Create network policies for ingress and egress to map incoming DSCP and EXP values to forwarding class and profile state and outgoing traffic from forwarding class and profile state to DSCP and EXP values.
Policies→Slope Policy Manager	Create slope parameters for access and network ports, and daughter cards.
Policies→Network Queue Policy Manager	Define the default buffer allocations for queues based on the queue's forwarding class.
Policies→Scheduler Policy Manager	Create scheduler policies to determine the order in which queues are serviced.
Policies→Acl IP Filter Manager	Create ACL IP filter policies to set the forward or drop action, as defined by the match criteria for incoming packets.
Policies→Acl MAC Filter Manager	Create ACL MAC filter policies to set the forward or drop action, as defined by the match criteria for incoming packets.

20.5 Policies procedures list

Table 20-4 lists the procedures to perform service management policies tasks.

For information about:

- routing and MPLS administrative group policies, see chapter 16
- alarm policies, see chapter 28
- file and accounting policies, see chapter 30
- mediation policies, see chapter 10
- poller policies, see chapter 6

Table 20-4 5620 SAM policies procedures list

Procedure	Purpose
To create an access ingress policy	Create one or more access ingress policies
To create an access egress policy	Create one or more access egress policies
To create a network policy	Create one or more network policies
To create a slope policy	Create one or more slope policies
To create a network queue policy	Create one or more network queue policies
To create a scheduler policy	Create one or more scheduler policies

(1 of 2)

Procedure	Purpose
To create an Acl IP filter policy	Create one or more ACL IP Filter policies
To create an Acl MAC filter policy	Create one or more MAC IP Filter policies
To distribute a policy	Distribute a policy or policies to a device or devices
To edit a policy	Edit a policy or entries within a policy
To delete a policy	Delete a policy or entries within a policy. When you delete a policy it is removed from the device and 5620 SAM database.
To copy or overwrite a policy	Copy or overwrite a policy
To synchronize a policy	Synchronize a policy or policies across the network
To remove an unassociated policy	Remove an unassociated policy or policies from a device or devices. The policies remain in the 5620 SAM database.

(2 of 2)

20.6 Policies procedures

Use the following procedures to perform 5620 SAM policies tasks. See the *7750 SR OS Services Guide* for more information about policy parameters.

Procedure 20-1 To create an access ingress policy

- 1 Choose Policies→Access Ingress Policy Manager from the 5620 SAM main menu.
The Access Ingress Policy Manager form opens.
- 2 Click on the Create SAP Ingress Policy button.
The policy form opens with the General tab button displayed.
- 3 Set the Configuration Action parameter.
- 4 Specify how you want to assign policy IDs.
 - a To have policy IDs automatically assigned, select the Auto-Assign ID check box.
 - b To manually assign a policy ID, deselect the Auto-Assign ID check box and enter an ID.

You can enter a name and description for the policy, if appropriate.
- 5 Specify a default forwarding class. The packets that are received on an ingress SAP using this policy are classified to the specified default forwarding class. See Table 20-2 for more information about forwarding classes.
- 6 Specify a priority for the packets that are received on an ingress SAP using this policy.

7 Click on the MAC Match Criteria or IP Match Criteria tab button to configure the match criteria.

8 Click on the Add button and configure the parameters.

9 Click on the Queues tab button.

The two default queues that cannot be deleted are displayed in the form: the default unicast traffic queue (ID 1) and the default multipoint traffic queue (ID 11).

10 Click on the Add button.

The Queue form opens with the General tab button displayed.

11 Specify a unique ID for the queue.

You can enter a name and description for the queue, if appropriate.

12 Set the Multicast parameter.

a To set the queue to multicast, set the parameter to true.

b To set the queue to unicast, set the parameter to false.

13 Set the Expedite parameter.

14 Choose a scheduler, if required.

The form refreshes and additional parameters appear.

15 Configure the newly displayed parameters, if required.

16 Click on the CIR/PIR tab button.

17 Configure the parameters.

Ensure that the CIR value is lower than the PIR value.

18 Click on the Burst Size tab button.

19 Configure the parameters.

Ensure that the Committed Burst Size value is lower than the Maximum Burst Size value.

20 Click on the OK button.

A confirmation dialog box appears.

21 Click on the OK button to close the dialog box.

The policy form reappears.

22 To configure additional queues, return to step 10. You can add up to 32 queues.

23 Click on the Forwarding Classes tab button.

24 Click on the Add button.

The forwarding class form opens.

- 25** Configure the parameters. You can create one entry for each of the eight forwarding class types.
- The Queue ID must be set to a unicast ID.
 - The Multicast, Broadcast, and Unknown IDs must be set to multicast IDs.
 - Click on the Select button to display a list of valid queues and to choose a queue.
 - Set the Queue ID to 0 if you want the default queue id to be used. The default id for unicast queues is 1. The default id for multicast, broadcast, unknown queues is 11.
- 26** Click on the OK button.
- A confirmation dialog box appears.
- 27** Click on the OK button to close the dialog box.
- The forwarding class form closes, and the policy form reappears.
- 28** 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, and precedence), or IP criteria and MAC criteria. Table 20-5 describes the options.

Table 20-5 Access ingress policy traffic mapping configuration options

Tab button	Use
Dot1p	Maps the Dot1p of the ingress traffic and ingress queue ID.
DCSP	Maps the DSCP of the ingress traffic and ingress queue ID.
Precedence	Maps the precedence of the ingress traffic and ingress queue ID.
IP Match Criteria	Maps the IP Match Criteria of the ingress traffic and ingress queue ID. This tab button is only configurable if you chose IP in step 7.
MAC Match Criteria	Maps the MAC Match Criteria of the ingress traffic and ingress queue ID. This tab button is only configurable if you chose MAC in step 7.

Perform the following substeps for each mapping that you want to configure.

- i** Click on the appropriate tab button.

The parameters are displayed.

- ii** Click on the Add button.

A Create form opens.

- iii** Configure the parameters.

If you configure the Protocol parameter under the IP Match Criteria tab button, when you choose TCP or UDP, additional parameters appear which can be configured.

If you configure the Frame type parameter under the MAC Match Criteria tab button, when you choose any option other than e802dot3, additional parameters appear which can be configured.

- iv** Click on the OK button to close the form.

A confirmation dialog box appears.

- v** Click on the OK button to close the dialog box.

The form closes and the policy form reappears.

- 29** Click on the Relations tab button to view a graphical representation of queue classification objects.
 - 30** Click on the Apply button to save the policy. The form is refreshed with additional buttons.
 - 31** 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.
 - 32** Close the Access Ingress Policy form. The Access Ingress Policy Manager form reappears.
 - 33** Click on the Search button to display the newly created policy or policies in the bottom panel of the form.
-

Procedure 20-2 To create an access egress policy

The following procedure describes how to create a policy.

- 1** Choose Policies→Access Egress Policy Manager from the 5620 SAM main menu.
The Access Egress Policy Manager form opens.
- 2** Click on the Create SAP Egress Policy button.
The Access Egress Policy form opens with the General tab button displayed.
- 3** Set the Configuration Action parameter.
- 4** Specify how you want to assign policy IDs.
 - a** To have policy IDs automatically assigned, select the Auto-Assign ID check box.
 - b** To manually assign a policy ID, deselect the Auto-Assign ID check box and enter an ID.

You can enter a name and description for the policy, if appropriate.

- 5** Click on the Queues tab button.
One default queue is displayed in the form.

- 6** Click on the Add button to add queues.
The Queue form opens with the General tab button displayed.
- 7** Enter a unique ID for the queue. You can enter a name and a description, if appropriate.
- 8** Set the Expedite parameter.
- 9** Choose a scheduler using the Select button.
Choose a scheduler from the list and click on the OK button.
- 10** Click on the Cir/Pir tab button.
- 11** Configure the parameters.
Ensure that the CIR value is lower than the PIR value.

See the “Subscriber Services” chapter in the *7750 SR OS Services Guide* for more information about adaptation rules.
- 12** Click on the Burst Size tab button.
- 13** Configure the parameters.
Ensure that the Committed Burst Size is lower than the Maximum Burst Size.
- 14** Click on the OK button.
The Queue form closes and the policy form reappears.
- 15** To create additional queues, return to step 6. You can create up to 8 queues.
- 16** Click on the Forwarding Classes tab button.
- 17** Click on the Add button.
The Forwarding Class form opens.
- 18** Configure the parameters. You can create one entry for each of the eight forwarding class types.
 - i** Choose a forwarding class.
 - ii** Enter a queue ID or click on the Select button to display a list of valid queues.
 - iii** Choose a dot1p parameter.
- 19** Click on the OK button to close the forwarding class form.
The forwarding class form closes and the Access Egress Policy form reappears with a list of the newly created forwarding classes displayed.
- 20** Click on the Apply button to save the policy. The form is refreshed with additional buttons.
- 21** 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.

- 22 Close the Access Egress Policy form. The Access Egress Policy Manager form reappears.
 - 23 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.
-

Procedure 20-3 To create a network policy

- 1 Choose Policies→Network Policy Manager from the 5620 SAM main menu.
The Network Policy Manager form opens.
- 2 Click on the Create Network Policy button.
The policy form opens with the General tab button displayed.
- 3 Set the Configuration Action parameter.
- 4 Specify how you want to assign policy IDs.
 - a To have policy IDs automatically assigned, select the Auto-Assign ID check box.
 - b To manually assign a policy ID, deselect the Auto-Assign ID check box and enter an ID.

You can enter a name and description for the policy if appropriate.
- 5 Set an ingress default forwarding class parameter.
- 6 Set an ingress default forwarding class profile parameter.
- 7 Set the Egress Remark parameter.
 - a To remark all packets on egress on the specified port, set the parameter to true.
 - b For all packets not to be remarked on egress on the specified port, set the parameter to false.
- 8 Click on the Egress Forwarding Classes tab button.

Eight default objects based on the eight forwarding classes, as described in Table 20-2, are displayed in the form. Configure the forwarding class parameters as required.
- 9 Double-click on a forwarding class.
The network forwarding class form opens.
- 10 Configure the parameters.
- 11 Click on the OK button.

- 12** 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 for LSP EXP Bits and Ingress DCSP. Table 20-6 describes the options.

Table 20-6 Network policy traffic mapping configuration options

Tab button	Use
LSP EXP Bits	Maps the LSP EXP Bits of the ingress traffic and ingress queue ID.
Ingress DCSP	Maps the DSCP of the ingress traffic and ingress queue ID.
Ingress Dot1p	Maps the Dot1p tag of the ingress traffic and ingress queue ID.

Perform the following substeps for each mapping that you want to configure.

- i** Click on the appropriate tab button.
The parameters are displayed.
 - ii** Click on the Add button.
A Create form opens.
 - iii** Configure the parameters.
 - iv** Click on the OK button to close the form.
The policy form reappears with the newly created object displayed.
- 13** Click on the Apply button to save the policy. The Network Policy form is refreshed with additional buttons.
- 14** 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.
- 15** Close the Network Policy form. The Network Policy Manager form reappears.
- 16** Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 20-4 To create a slope policy

- 1** Choose Policies→Slope Policy Manager from the 5620 SAM main menu.
The Slope Policy Manager form opens.
- 2** Click on the Create Slope Policy button. The slope policy form with the General tab button appears, as shown in Figure 20-13.

Figure 20-13 Slope policy form - General

Policy, Global Policy - [Create]

General Slopes Definitions

Configuration Action: Merge With Existing

Displayed Name: [] Description: []

Time Average Factor (weight): 7

Reset OK Cancel Apply

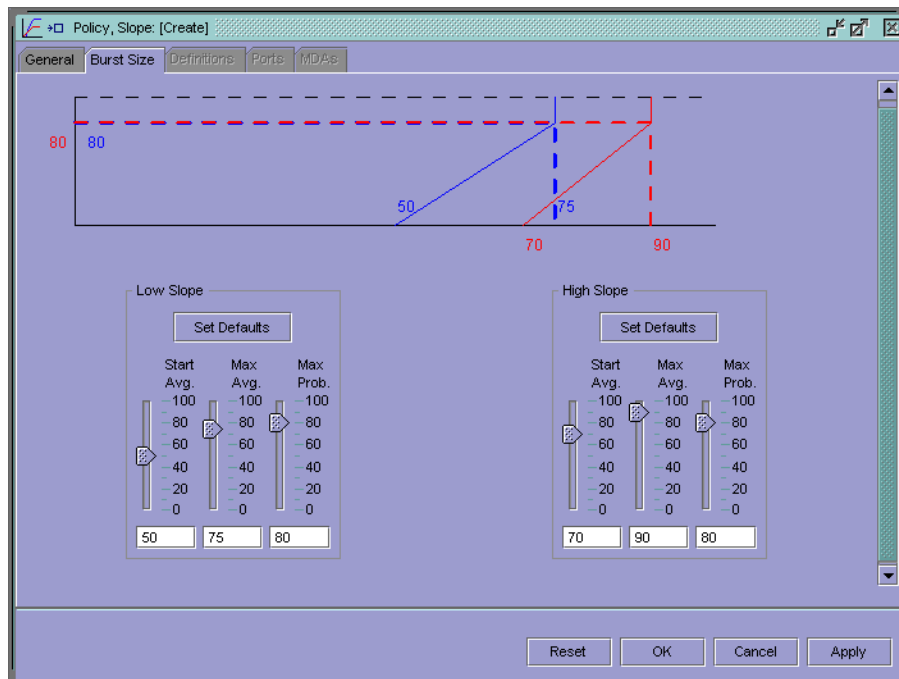
Configure the parameters.

- i Set the Configuration Action parameter. The options are:
 - Merge with Existing
 - Overwrite Existing
 - Fail If Exists
- ii Specify a name for the policy.
- iii Specify a description for the policy.
- iv Specify a value for the Time Average Factor (weight) parameter. The range is 0 to 15.

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.

- 3 Click on the Burst Size tab button. The Burst Size form appears, as shown in Figure 20-14.

Figure 20-14 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 section 20.2 for more information.

- i Configure the Start Avg., Max. Avg., and the Max Prob. parameters for the High Slope.
 - ii Configure the Start Avg., Max. Avg, and the Max Prob. parameters for the Low Slope.
- 4 Click on the Apply button to save the policy. The Slope Policy form is refreshed with additional buttons.
 - 5 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.
 - 6 Close the Slope Policy form. The Slope Policy Manager form reappears.
 - 7 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 20-5 To create a network queue policy

- 1 Choose Policies→Network Queue Policy Manager from the 5620 SAM main menu.
The Network Queue Policy Manager form opens.

- 2 Click on the Create Network Queue Policy button.

The Network queue policy form with the General tab button appears, as shown in Figure 20-15.

Figure 20-15 Network Queue Policy form - General

The screenshot shows a software window titled "Policy, Global Policy- [Create]". It features a tabbed interface with tabs for "General", "Queues", "Forwarding Classes", "Definitions", "Ports", and "MDAs". The "General" tab is selected. The main area contains a "Configuration Action" dropdown menu with "Merge With Existing" selected. Below this are two text input fields: "Displayed Name" (highlighted in yellow) and "Description". At the bottom right, there are four buttons: "Reset", "OK", "Cancel", and "Apply".

Configure the parameters.

- i Set the Configuration Action parameter. The options are:
 - Merge with Existing
 - Overwrite Existing
 - Fail If Exists
 - ii Specify a name for the policy.
 - iii Specify a description for the policy.
- 3 Click on the Queues tab button. The Network queue form with the Queues tab appears, as shown in Figure 20-16.

Figure 20-16 Network queue policy form - Queues

ID	Displayed Name	Description	Pool Name	Ctr (%)	Pir (%)
1	entry-1		N/A	0	100
2	entry-2		N/A	25	100
3	entry-3		N/A	25	100
4	entry-4		N/A	25	100
5	entry-5		N/A	100	100
6	entry-6		N/A	100	100
7	entry-7		N/A	10	100
8	entry-8		N/A	10	100

Eight default queues are displayed in the form. Configure the queues as required.

- i Choose a queue and click the Edit button. The Queue configuration form General tab button appears, as shown in Figure 20-17.

Figure 20-17 Queue configuration form - General

The screenshot shows a window titled "Entry, entry-2 [Create]". It has three tabs: "General", "CIR/PIR", and "Burst Size". The "General" tab is selected. The form contains the following fields:

- ID:
- Displayed Name:
- Description:

At the bottom right, there are four buttons: "Reset", "OK", "Cancel", and "Apply".

- ii Configure the General tab button queue parameters.
 - Modify the ID, if required.
 - Modify the Displayed Name, if required.
 - Enter a Description.
 - iii Click on the CIR/PIR tab button. Configure the parameters.
 - Modify the Cir, if required. The range is 0 to 100%.
 - Modify the Pir, if required. The range is 0 to 100%.
 - iv Click on the Burst Site tab button. Configure the parameters.
 - Modify the Committed Burst Size, if required. The range is 0 to 100%.
 - Modify the Maximum Burst Size, if required. The range is 0 to 100%.
 - Modify the High Priority Reserved, if required. The range is 0 to 100%.
 - v Click on the OK button to close the queue configuration form.
- 4 Click on the Forwarding Classes tab button. The Network queue policy with Forwarding Classes tab appears, as shown in Figure 20-18.

Figure 20-18 Network queue policy form - Forwarding Classes

Forwarding Class	Queue ID
be	1
l2	2
af	3
l1	4
h2	5
ef	6
h1	7
nc	8

Eight default objects based on the eight forwarding classes, as described in Table 20-2, are displayed in the form. Configure the forwarding class parameters as required.

- i Choose a forwarding class and click the Edit button. The forwarding class form appears, as shown in Figure 20-19.

Figure 20-19 Forwarding class form

- ii Modify the Queue ID parameter, if required.
 - iii Click on the OK button to close the forwarding class configuration form.
- 5 Click on the Apply button to save the policy. The Network Queue Policy form is refreshed with additional buttons.

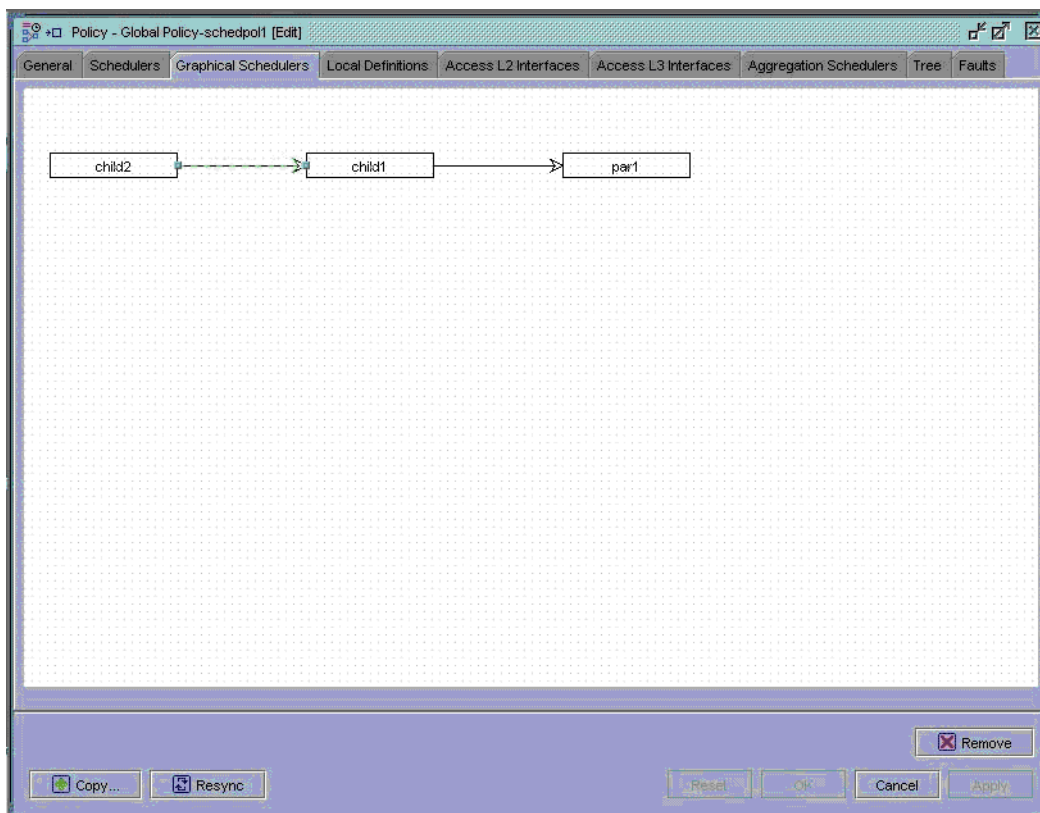
- 6 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.
 - 7 Close the Network Queue Policy form. The Network Queue Policy Manager form reappears.
 - 8 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.
-

Procedure 20-6 To create a scheduler policy

- 1 Choose Policies→Scheduler Policy Manager from the 5620 SAM main menu.
The Scheduler Policy Manager form opens.
- 2 Click on the Create Scheduler Policy button.
The policy form opens with the General tab button displayed.
- 3 Set the Configuration Action parameter.
- 4 Enter a name for the policy.
- 5 Click on the Schedulers tab button.
- 6 Click on the Add button.
The Entry form opens.
- 7 Enter a unique name for the scheduler. Names can be up to 32 characters.
The scheduler defines bandwidth control that limits each child (other schedulers and queues) that are associated with the scheduler.
- 8 Specify the tier. A tier 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.
When creating children or grandchildren schedulers, you must specify tier 2 or tier 3 before choosing a parent scheduler.
- 9 If you are creating a child scheduler, you must specify the parent scheduler name to be associated with a level 2 or 3 tier. Click on the Select button to display a list of valid parent schedulers.
- 10 Configure the parameters.
 - a Configure the Summed CIR parameter.
 - b If you are creating a child scheduler, configure the parent scheduler parameters.
- 11 Click on the OK button to close the Entry form.

- 12 To add additional schedulers to the policy, return to step 6.
- 13 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 20-20.

Figure 20-20 Hierarchical view of schedulers with a policy form - Graphical Schedulers



- 14 Click on the Apply button to save the policy. The Scheduler Policy form is refreshed with additional buttons.
- 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.
- 16 Close the Scheduler Policy form. The Scheduler Policy Manager form reappears.
- 17 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 20-7 To create an aggregation scheduler

You can create an aggregation scheduler when you have created two or more scheduler policies. See “Hierarchical schedulers” in section 20.2 for more information.



Note — You can also create an aggregation scheduler during the configuration of subscriber services.

- 1 Create two or more scheduler policies, as described in Procedure 20-6.
 - 2 Choose Service Management→Manage Subscribers/Service from the 5620 SAM main menu.

The Subscriber Manager form opens.
 - 3 Search for available subscribers.
 - 4 Choose a subscriber.
 - 5 Click on the Edit button.

The subscriber policy form opens.
 - 6 Click on the Aggregation tab button.
 - 7 Click on the Add button.

The Create Aggregation Scheduler form opens at the Define Name step.
 - 8 Choose a name and description for the aggregation scheduler.
 - 9 Click on the Next button. The Select Site form opens.

Choose a site.
 - 10 Click on the Next button. The Select Assignment Scope form opens.

Choose Card or Port from the drop-down menu.
 - 11 Click on the Next button. The Select Card or the Select Port form opens.

Choose a card or a port using the Select button.
 - 12 Click on the Next button. The Select Ingress and Egress Scheduler Policies form appears.

Click on the Select buttons to choose the ingress and egress scheduler policies.
 - 13 Click on the Finish button.

The aggregation scheduler is listed in the Aggregation tab button of the subscriber form.
-

Procedure 20-8 To create an Acl IP filter policy

- 1 Choose Policies→Acl IP Filter Manager from the 5620 SAM main menu.
The Acl IP Filter Manager form opens.
- 2 Click on the Create ACL IP Filter button.
The IP filter form opens with the General tab button displayed.
- 3 Set the Configuration Action parameter.
- 4 Specify how you want to assign filter IDs.
 - a To have filter IDs automatically assigned, select the Auto-Assign ID check box.
 - b To manually assign a filter ID, deselect the Auto-Assign ID check box and enter an ID.
- 5 Enter a name and description for the policy.
- 6 Choose a default action from the drop-down list. The default action specifies the action to be applied to packets when no action is specified in the IP filter entries or when the packets do not match the specified criteria.
- 7 Click on the Filter Entries tab button.
- 8 Click on the Add button.
The IP filter entry form opens.
- 9 Specify how you want entry IDs assigned. Each entry ID must be unique. The entry ID determines the order amongst all entry IDs, within a specific filter ID, in which the matching criteria specified in the collection is compared. Packets are compared to entry IDs in an ascending order.
 - a To have IDs automatically assigned to the entry, select the Auto-Assign ID check box.
 - b To manually assign an ID to the entry, deselect the Auto-Assign ID check box and enter an ID.

You can enter a name and description if appropriate.
- 10 Click on the Filter Properties tab button.
- 11 Specify the Action parameter. The options are drop, forward, or default.
If you specify Forward, the Next Hop Routing tab button appears.
 - i Click on the Next Hop Routing tab button.
 - ii Configure the parameters.
- 12 Specify the Protocol parameter.
If you specify ICMP, TCP, or UDP, additional parameters appear in the bottom portion of the form.

- 13 Configure the Match Criteria. Matches for the filter can be based on:
 - DSCP
 - source and destination IP addresses
 - subnet masks of IP addresses
 - IP options
 - fragments
 - 14 Configure the additional Protocol related parameters, if required.
 - 15 Click on the Cflowd tab button.
 - 16 Configure the Cflowd parameters.
 - 17 Click on the OK button.

The IP filter entry form closes and a confirmation dialog box appears.
 - 18 Click on the OK button to close the dialog box.

The IP filter form reappears with the newly created filter entry or entries displayed.
 - 19 To add additional filter entries, return to step 8.
 - 20 Click on the Apply button to save the policy. The IP Filter form is refreshed with additional buttons.
 - 21 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.
 - 22 Close the IP Filter form. The Acl IP Filter Manager form reappears.
 - 23 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.
-

Procedure 20-9 To create an Acl MAC filter policy

- 1 Choose Policies→Acl MAC Filter Manager from the 5620 SAM main menu.

The Acl MAC Filter Manager form opens.
- 2 Click on the Create ACL MAC Filter button.

The MAC filter form opens with the General tab button displayed.
- 3 Set the Configuration Action parameter.
- 4 Specify how you want to assign filter IDs.
 - a To have filter IDs automatically assigned, select the Auto-Assign ID check box.
 - b To manually assign a filter ID, deselect the Auto-Assign ID check box and enter an ID.

You can enter a name and description for the policy, if appropriate.

- 5 Choose a default action from the drop-down list. The default action 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.
- 6 Click on the Filter Entries tab button.
- 7 Click on the Add button.

The Mac filter entry form opens.

- 8 Specify how you want entry IDs assigned. Each entry ID must be unique. The entry ID determines the order of all entry IDs, within a specific filter ID, in which the matching criteria specified in the collection is compared. Packets are compared to entry IDs in an ascending order.
 - a To have IDs automatically assigned to the entry, select the Auto-Assign ID check box.
 - b To manually assign an ID to the entry, deselect the Auto-Assign ID check box and enter an ID.

You can enter a name and description, if appropriate.

- 9 Click on the Filter Properties tab button.
- 10 Specify the Action parameter to either drop, forward or default. This parameter specifies the action performed on the filtered packet.
- 11 Specify the Frame Type parameter. If you specify e802do2LLC, e802dot2SNAP, or Ethernet II, additional parameters appear in the bottom portion of the form.
- 12 Configure the Match Criteria.

The match criteria can be based on a number of matching actions, for example, the source MAC address and the source MAC address mask.

- 13 Scroll down and configure the additional the Frame Type related parameters, if required.
- 14 Click on the OK button.

The MAC filter entry form closes and a confirmation dialog box appears.

- 15 Click on the OK button to close the dialog box.

The Mac filter form reappears with the newly created filter entry or entries displayed.

- 16 To add additional filter entries, return to step 7.
- 17 Click on the Apply button to save the policy. The MAC Filter form is refreshed with additional buttons.
- 18 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.
- 19 Close the MAC Filter form. The Acl MAC Filter Manager form reappears.

- 20 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.
-

Procedure 20-10 To distribute a policy

Policies used by network resources can be manually distributed using the following procedure. Policies are also distributed to a device when the policy is assigned to a resource on that device.

- 1 Choose Policies→*Policy Manager* from the 5620 SAM main menu, where *Policy Manager* is the type of policy that you want to distribute.
The policy manager form opens.
 - 2 Click on the Search button.
A list of search results is displayed.
 - 3 Choose the policy or policies that you want to distribute.
 - 4 Click on the Distribute button.
The Distribute form appears.
 - 5 Click on the Selected radio button to choose from the listed devices.
 - 6 Choose a row or rows from the Available Nodes list.
 - 7 Click on the right arrow button.
The chosen device or devices move to the panel on the right side of the form.
 - 8 Click on the Distribute button. The policy is distributed to the device or devices.
 - 9 Close the Distribute form.
The policy manager form reappears.
 - 10 View the devices that a policy is distributed to.
 - i Choose the policy.
 - ii Click on the Edit button.
The policy form opens.
 - iii Click on the Local Definitions tab button.
The device information for the chosen policy is displayed.
 - 11 To distribute additional policies, return to step 3.
-

Procedure 20-11 To edit a policy

You can change existing policies and entries within policies using the 5620 SAM GUI or the CLI. The changes are applied immediately to all resources where the policy is applied.

- 1 Choose Policies→*Policy Manager* from the 5620 SAM main menu, where *Policy Manager* is the type of policy that you want to edit.

The policy manager form opens.

- 2 Click on the Search button.

A list of search results is displayed in the bottom panel of the form.

- 3 Choose the policy that you want to edit.

- 4 Click on the Edit button.

The policy configuration form opens.

- 5 Configure the parameters, as required.

- 6 Click on the OK button to save the changes.

A confirmation dialog box appears.

- 7 Click on the Yes button to close the dialog box.

The policy configuration form closes and the policy manager form reappears.

Procedure 20-12 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 an SAP or IP interface, the policy association reverts to the default policy (ingress or egress policy ID 1).

A QoS or ACL 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.

- 1 Choose Policies→*Policy Manager* from the 5620 SAM main menu, where *Policy Manager* is the type of policy that you want to delete.

The policy manager form opens.

- 2 Click on the Search button.

A list of search results is displayed in the bottom panel of the form.

- 3 Choose the policy that you want to delete.

- 4 Click on the Remove button to delete the policy.

A confirmation dialog box appears.

- 5 Click on the Yes button.

The dialog box and the policy configuration form close and the policy manager form reappears. The policy is removed from the policy list.

Procedure 20-13 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.

Instead of overwriting an existing policy, you can merge components of a policy with another by using the merge option.

Procedure 20-14 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 20-10.

- 1 Choose Policies→*Policy Manager* from the 5620 SAM main menu, where *Policy Manager* is the type of policy that you want to synchronize.

The policy manager form opens.

- 2 Click on the Search button.

A list of search results is displayed.

- 3 Choose the policy or policies that you want to synchronize.

- 4 Click on the Synchronize button.

The Synchronize form appears.

- 5 Choose the device or devices to which the policy is to be distributed from the Available Nodes list.

- 6 Click on the right arrow button.

The chosen device or devices move to the panel on the right side of the form.

- 7 Click on the Synchronize button.

- 8 Click on the Cancel button to close the form.
-

Procedure 20-15 To remove an unassociated policy

You can use the free unused option to remove the policies that have no associations from one or more devices. When you perform this procedure, the policy is deleted from the devices where the policy is not associated with a particular service or router interface. When a policy is created and distributed to a device, it can subsequently be associated with a particular service or router interface. Until that association is performed, the policy is not in use although it remains on the device.

When you remove unassociated policies from one or more devices, the policy remains accessible from the 5620 SAM and remains in the database.

- 1 Choose Policies→*Policy Manager* from the 5620 SAM main menu, where *Policy Manager* is the type of policy that you want to remove.

The policy manager form opens.

- 2 Click on the Search button.

A list of search results is displayed.

- 3 Choose the policy or policies that you want to remove.

- 4 Click on the Free Unused button.

The policy form appears.

- 5 Click on the Cancel button to close the form.
-

21 — Subscriber configuration and management

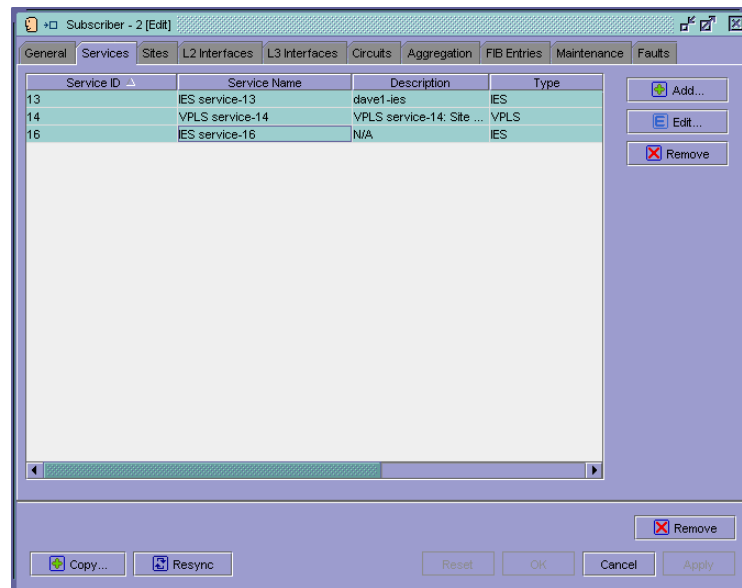
- 21.1 Subscriber overview 21-2**
- 21.2 Workflow to configure and manage subscribers 21-2**
- 21.3 Subscriber menu 21-3**
- 21.4 Subscriber configuration and management procedures list 21-3**
- 21.5 Subscriber configuration and management procedures 21-3**

21.1 Subscriber overview

The 5620 SAM allows you to manage subscribers. Subscribers are the customers that pay for services such as VPLS. The terms customers and subscribers are used synonymously.

From the Subscriber Manager form, you can configure and monitor services, resources, alarms, and statistics for a subscriber. Figure 21-1 shows a subscriber form with the Services tab button selected. In this example, Subscriber 2 is using three services. From the other tab buttons on the form, you can view information about the subscriber's account, for example the circuits that forward customer traffic.

Figure 21-1 Subscriber form - Services



Each subscriber is associated with a subscriber ID. The basic required subscriber parameter is the subscriber ID, which is assigned when the subscriber account is created. The subscriber ID is used when modifying subscriber information on the node using CLI. When associating a subscriber with a service, you can use the subscriber ID or the listed name of subscribers.

The subscriber ID is used in service creation. It is often the first step as, in most cases, new services are added to existing subscribers. A subscriber can have more than one associated service.

21.2 Workflow to configure and manage subscribers

- 1 Create subscribers that will purchase and use services.
 - Configure or modify key customer contact and billing information.
 - Assign or associate equipment or resource to the customers, as appropriate.
- 2 Create or modify services for subscribers, such as VLL.

- 3 Monitor or troubleshoot subscribers based on SLAs between the subscriber and the service provider.
 - Retrieve subscriber information and contact the customer when service problems or maintenance windows occur.
 - Use 5620 SAM tools to monitor alarms that are raised against subscriber-assigned equipment or services.
 - Perform diagnostics as appropriate to troubleshoot problems.

21.3 Subscriber menu

Table 21-1 lists the subscriber menu.

Table 21-1 5620 SAM subscriber menu

Menu option	Function
Service Management→Manage Subscribers/Services	Manage subscribers and services.

21.4 Subscriber configuration and management procedures list

Table 21-2 lists the procedures to configure and manage subscribers.

Table 21-2 5620 SAM subscriber procedures list

Procedure	Purpose
To create subscribers	Create one or more subscribers to use a service, such as VPLS.
To modify and manage subscriber information	Modify subscriber information based on changes to the services used by the customer and to manage the customer account.
To delete subscribers	Delete a subscriber.
To view subscriber maps	View a topology map of all devices and services used by the subscriber.

21.5 Subscriber configuration and management procedures

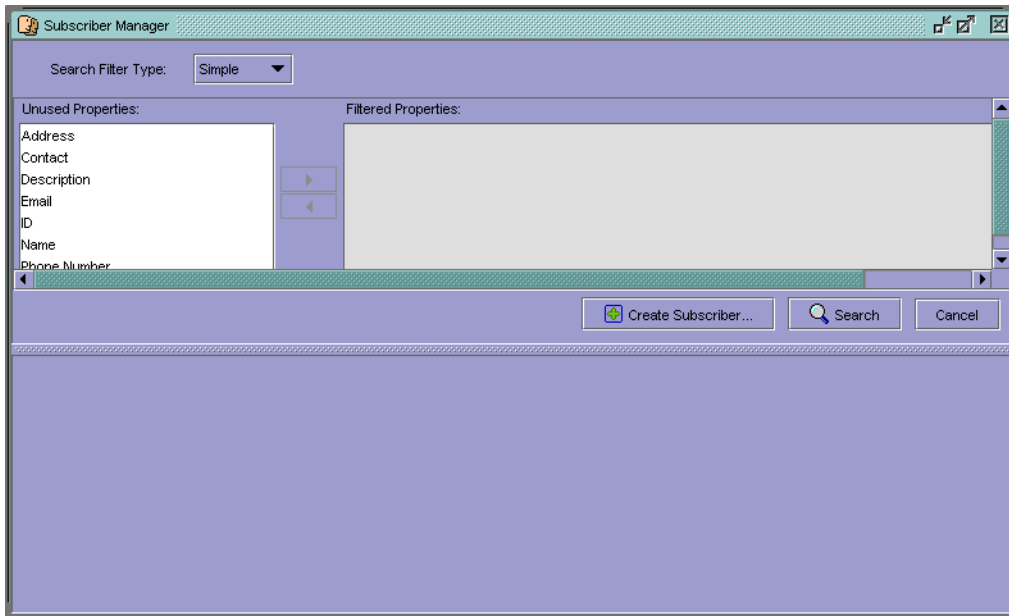
The following procedures describe how to configure and manage subscribers.

Procedure 21-1 To create subscribers

- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu.

The Subscriber Manager form opens, as shown in Figure 21-2.

Figure 21-2 Subscriber Manager form



- 2 Click on the Create Subscriber button.

The Subscriber (Create) form opens with General tab button selected, as shown in Figure 21-3. Contact and billing information about the subscriber appears under the General tab.

Figure 21-3 Subscriber form - General

The screenshot displays the 'Subscriber, [Create]' form in the 'General' tab. The form contains the following fields and options:

- ID:** A text input field containing the value '0'. To its right is a checked checkbox labeled 'Auto-Assign ID'.
- Name:** A text input field containing 'Name of the company buying your service'.
- Description:** A text input field containing 'Place a description of the subscriber purchasing services here'.
- Address:** A text input field containing 'Contact or billing address information'.
- Phone Number:** A text input field containing '7-777-777-7777'.
- Email:** A text input field containing 'ntact@companyname.com'.
- Contact:** A text input field containing 'Contact name'.

At the bottom of the form are four buttons: 'Reset', 'OK', 'Cancel', and 'Apply'. The background shows a network topology tree with the following structure:

- Network
 - Router pc23 (10.1.1.23)
 - Chassis 1 (4-Slot), pc23
 - Slot 01 (1 x 10-Gig MDA IOM), OK
 - Slot 02 (1 x 10-Gig MDA IOM), Remo
 - Slot 03 (2 x 10-Gig MDA IOM), Remo
 - Slot A (CPM / Switch Fabric), OK
 - leg 1, Oper Down
 - leg 2, Oper Down
 - Router pc30 (10.1.1.30)
 - Router pc31 (10.1.1.31)

The bottom status bar shows 'admin is logged in', 'GUI Activity Check Disabled', and the date 'Mon Dec 22 12:56:39 EST 2003'.

- 3 Enter the customer information, including contact information, so that the customer can be contacted if there is a service or equipment problem.
- 4 Specify how you want IDs assigned to the subscriber.
 - a To have the 5620 SAM automatically assign a subscriber ID, select the Auto-Assign ID check box.
 - b To manually assign a subscriber ID, deselect the Auto-Assign ID check box.
- 5 Click on the Apply button to save the subscriber information.

Procedure 21-2 To modify and manage subscriber information

You can view and modify an inventory of all the services, interfaces, circuits, and other information that is associated with each subscriber.

- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu.
The Subscriber Manager form opens.
- 2 Search for the subscriber whose information you want to change.

The search results are displayed in the bottom panel of the form.

- 3 Choose the subscriber and click on the Edit button.

The Subscriber form appears.

- 4 View or modify the information for the subscriber. Figure 21-1 shows the Subscriber form with the Services tab selected.

Each tab lists parameters you can view or modify, or functions that you can perform, related to subscriber management.

For example, to make a change to a service that is associated with the subscriber, you can click on the Services tab and view all the services subscribed to by the customer. You can then create a new service or edit an existing service to change the parameters of the service to meet the customer's new requirements. The following information appears for existing subscribers:

- The General tab lists the subscriber ID, the subscriber name, and contact information.
 - The Services tab lists the services used by the subscriber. You can change existing services, or add new services.
 - The Sites tab lists PE devices used by the subscriber for their services.
 - The L2 Interfaces tab lists Layer 2 interfaces used by the subscriber.
 - The L3 Interfaces tab lists IP Layer 3 interfaces used for Internet-based services.
 - The Circuits tab (circuits are VC IDs bound to service tunnels) lists the circuits used by the subscriber. You can use the Circuit tab Add Spoke button to create access spoke circuits for HVPLS, as described in chapter 24.
 - The Aggregation tab lists the policies used to perform rate limiting across queues of multiple access interfaces.
 - The Address tab lists addresses used by the subscriber.
 - The Forwarding Control tab lists the learned MAC addresses of the services that use FIBs and spanning tree protocol information.
 - The Maintenance tab lists OAM diagnostics that can be performed to diagnose service problems. See chapter 29 for more information about performing OAM diagnostics.
 - The Faults tab lists all alarms correlated against subscribers
- 5 Modify subscriber information as appropriate:
 - a To modify subscriber services or equipment, such as interfaces used for the service:
 - i Click on the appropriate tab button on the subscriber form.
 - ii Choose the appropriate row from the list.
 - iii Click on the Edit button to open the configuration form and edit any of the data listed in step 4.



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.

22 — Service management overview

22.1 Service management overview 22-2

22.2 Access interfaces 22-6

22.3 Sample network configuration using HQoS 22-7

22.1 Service management overview

The 5620 SAM supports the configuration of four connectivity services:

- VLL service
- VPLS
- IES
- VPRN service

The benefits of the 5620 SAM service model include:

- end-to-end service configuration on the 5620 SAM using a sequence of configuration forms and steps
- template-based creation of policies which specify the classification, policing, shaping, and marking of traffic handled by the managed devices. Policies can be used by multiple services.
- closely-integrated fault management
- closely-integrated OAM tools
- changes can be made to a single service component (such as a service, service site, tunnel, circuit, or interface) rather than multiple ports on multiple devices
- tunnel configurations and transport are independent of the services that they carry

Figure 22-1 shows a 5620 SAM service configuration form with the Define Service Type parameters displayed.

Figure 22-1 Service configuration form - Define Service Type form

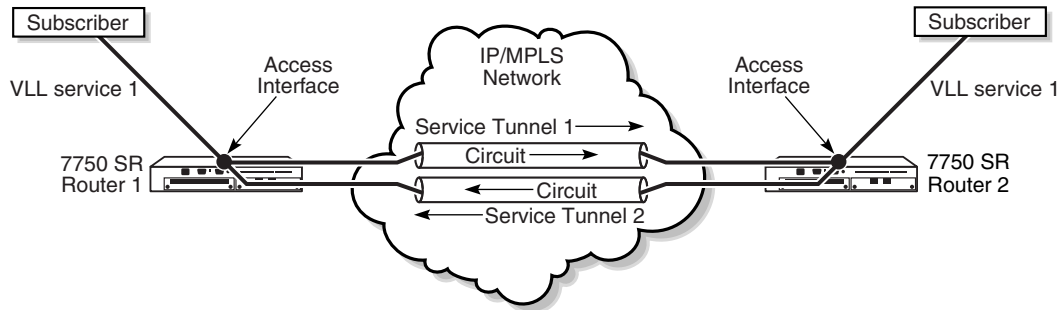
The screenshot shows a web-based configuration form titled "Define Service Type". The form is set against a light purple background. It contains the following fields and controls:

- Service ID:** A text input field containing the value "0". To its right is a checked checkbox labeled "Auto-Assign ID".
- Service Name:** A text input field that is currently empty.
- Description:** A text input field that is currently empty.
- Type:** A dropdown menu with "VLL" selected and a downward-pointing arrow.

For distributed VLL service and VPLS, devices are deployed at the provider edge. Customer traffic is fed into the service via access interfaces. The traffic is transported across an IP and/or IP/MPLS provider core network in unidirectional service tunnels that are created using GRE or MPLS LSPs. Many services can use the same tunnel.

A local VLL service or VPLS can also be configured. A local VLL service consists of two access interfaces on the same node. A local VPLS consists of multiple access interfaces on the same node. Figure 22-2 shows a sample distributed VLL service.

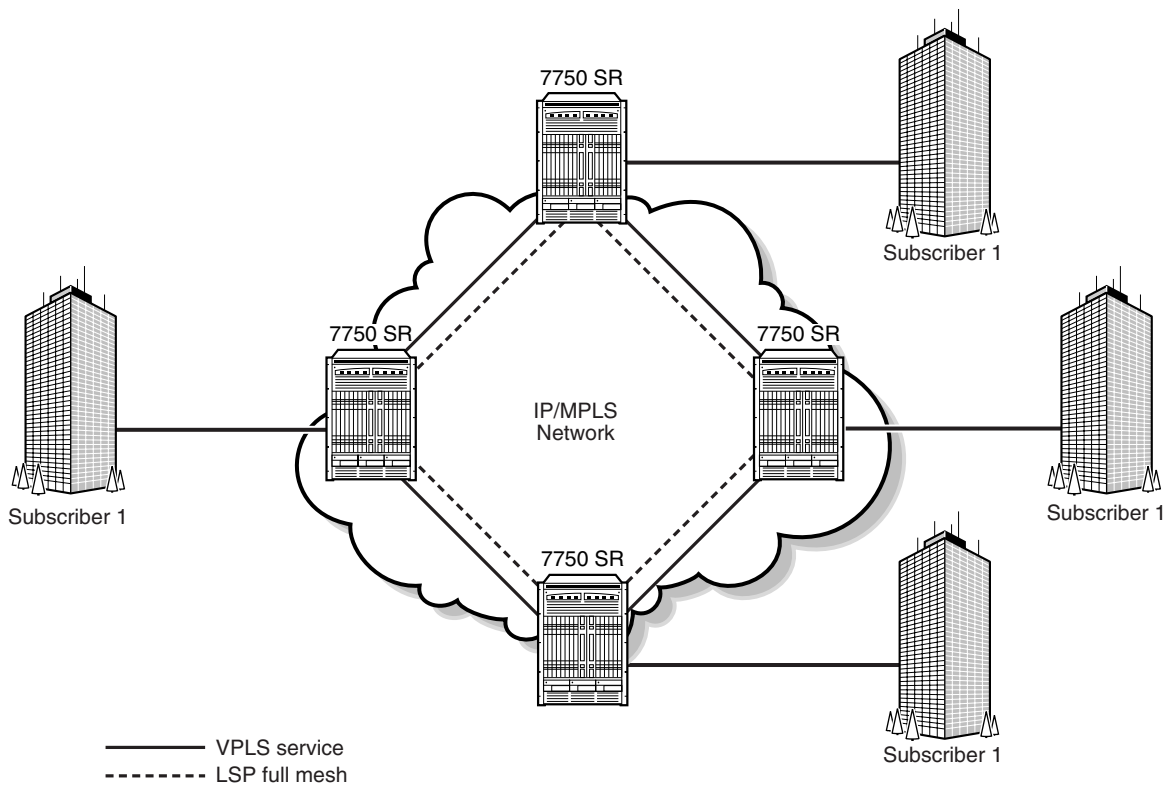
Figure 22-2 Sample distributed VLL service



17187

Figure 22-3 shows a sample distributed VPLS.

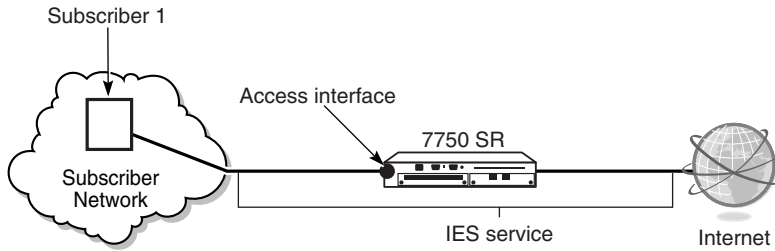
Figure 22-3 Sample distributed VPLS



17240

For IES, the managed devices are deployed at the provider edge and customer traffic enters the service via access interfaces. IES is a routed connectivity service where the subscriber communicates with an IP router interface to send and receive Internet traffic. Figure 22-4 shows a sample IES.

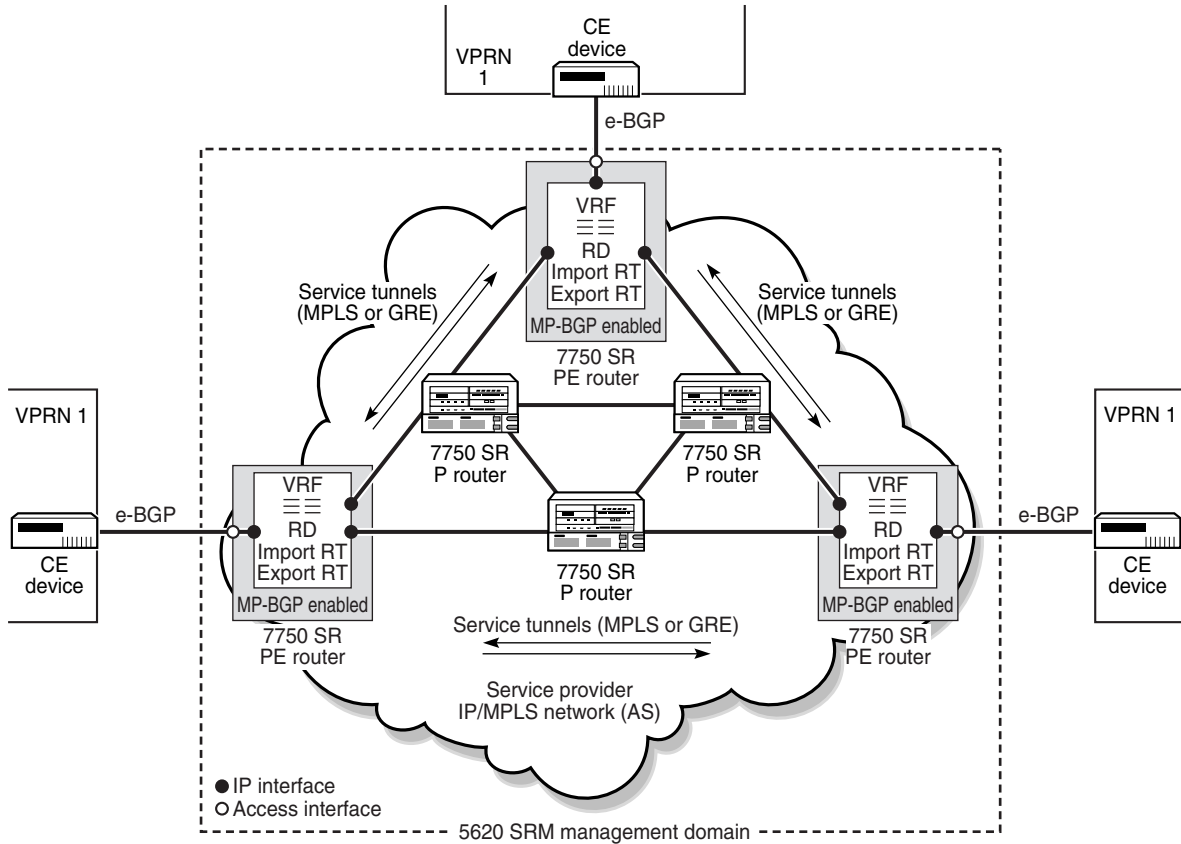
Figure 22-4 Sample IES



17239

For VPRN services, the managed devices can be deployed as a provider edge or provider core router. Data and distributing routing information are forwarded across an IP/MPLS service provider core network. Figure 22-5 shows a sample VPRN service.

Figure 22-5 Sample VPRN service



17333

Table 22-1 describes the high-level tasks that are required to configure a service. The tasks that you perform depend on your network requirements and the service that you are configuring.

Table 22-1 Configuring services

Task	Subtask	5620 SAM menu option	Information
Hardware configuration	Configure: <ul style="list-style-type: none"> • Devices • Daughter cards • Cards • Ports 	Equipment→Equipment Manager	See chapter 14 for more information about using the navigation tree. See chapter 15 for more information about using the equipment manager.
	Configure access buffer policies	Policies→Slope Policy Manager	See chapter 20 for more information.
	Configure network buffer policies	Policies→Network Queue Policy Manager	

(1 of 2)

Task	Subtask	5620 SAM menu option	Information
Network configuration	Configure routing	Equipment→Equipment Manager or select an object from the navigation tree.	See chapter 16 for more information.
	Configure LSPs	Topology→MPLS Path Manager Topology→LSP Manager	See chapter 18 for more information.
	Configure service tunnels	Topology→Service Tunnel Manager	
	Configure network policies	Policies→Network Policy Manager	See chapter 20 for more information.
Service-related policy configuration	Configure access ingress policies	Policies→Access Ingress Policy Manager	See chapter 20 for more information about policies.
	Configure access egress policies	Policies→Access Egress Policy Manager	
	Configure scheduling policies	Policies→Scheduler Policy Manager	
	Configure accounting policies	Policies→Accounting Policy Manager	
	Configure access list policies	Policies→Acl IP Filter Manager Policies→Acl MAC Filter Manager	
Subscriber configuration	—	Service Management→Manage Subscribers/Services	You specify the subscriber for a service when you configure the service.
Service configuration	Create VLL service Create VPLS Create IES Create VPRN	Service Management→Create Service You can also create a service for a subscriber by listing subscribers from the Manage Subscribers/Services form and choose a subscriber; click on the Services tab to configure the service.	Depending on the service, you must specify the following when you configure the service: <ul style="list-style-type: none"> • Subscriber • Service type • Sites (routers) • Access ports • Tunnels • Circuits • Policies <p>See chapter 23 for more information about VLL services. See chapter 24 for more information about VPLS. See chapter 25 for more information about IES. See the <i>7750 SR OS Services Guide</i> for more detailed information about VLL, VPLS, IES, and VPRN services.</p>

(2 of 2)

22.2 Access interfaces

Each subscriber service is configured with at least one access interface, which is also called a SAP. The access interface identifies the customer interface point for a service on the managed device.

A Layer 2 or Layer 3 access interface is uniquely identified by the:

- 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 subscriber or for multiple subscribers.

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. 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 given 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 (either administratively or operationally), access interfaces on that port/channel will be operationally out of service.

See the *7750 SR OS Services Guide* for more detailed information about access interfaces.

22.3 Sample network configuration using HQoS

The 5620 SAM supports the configuration of HQoS scheduling mechanisms. HQoS provides the ability to rate limit across multiple queues from single or multiple access interfaces for a given customer.

The building blocks for HQoS include:

- Access ingress and egress policies. These QoS policies specify how subscriber traffic is mapped into queues, and specify queue classification, queue parameters and marking.

Participation in access ingress and egress policies is defined when access interfaces are configured or modified.

- Scheduler policies. A scheduler policy defines a hierarchy of virtual schedulers that govern how queues are scheduled.

An aggregation scheduler can be used by an access interface directly, or by scheduler groups. When it is used by an access interface directly, the scheduler policy governs the overall rate limiting across all queues on the interface.

When the aggregation scheduler is used by an aggregation scheduler group, the scheduler policy defines the scheduling of all service queues from all participating access interfaces. An aggregation scheduler group spans access interfaces on a port or card for a specific subscriber.

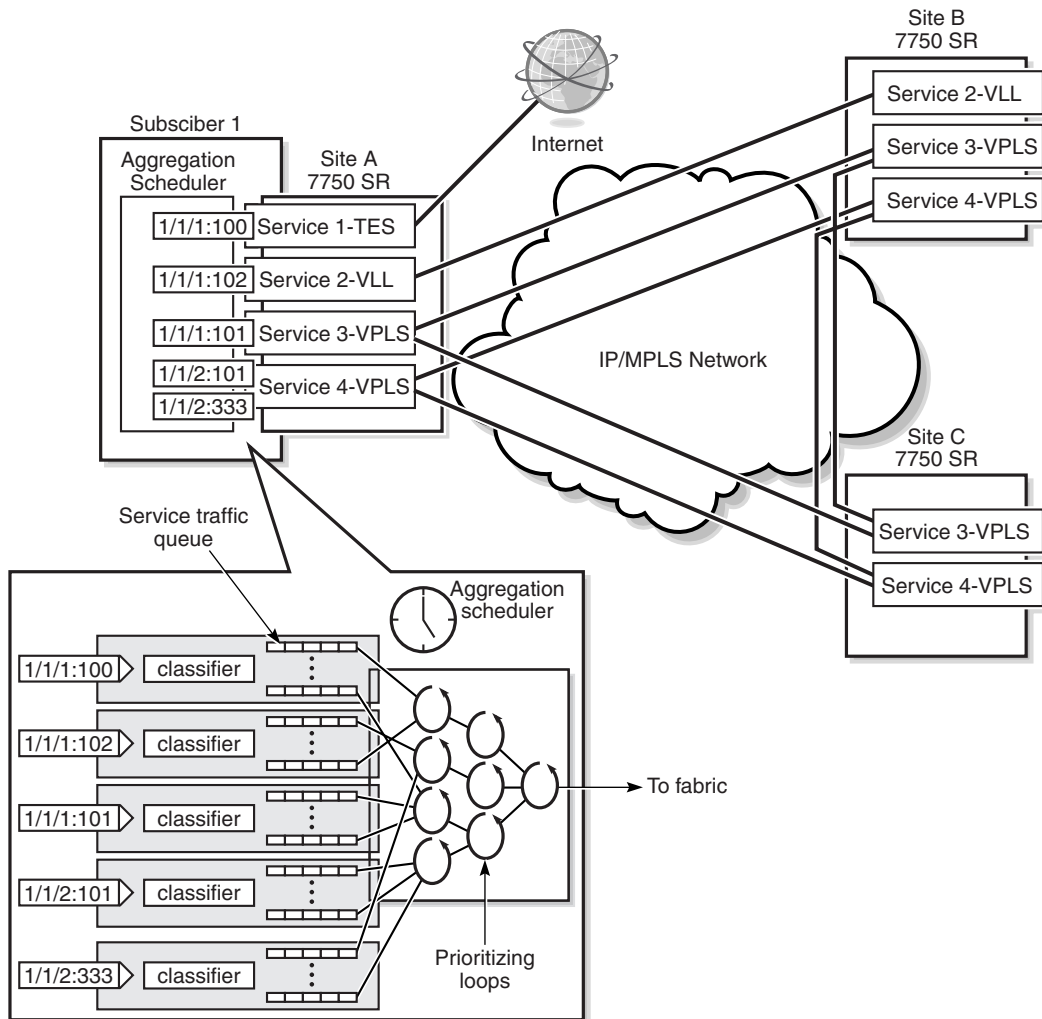
If a scheduler policy is not specified for an access interface, rate limiting is specified by the values specified in the queue.

Participation in scheduler policies is defined when access interfaces are configured or modified.

See chapter 20 for more information about policies on the 5620 SAM. See the *7750 SR OS Services Guide* for more detailed information about HQoS.

Figure 22-6 shows a sample service configuration using HQoS.

Figure 22-6 Sample service configuration using HQoS



17238

In this configuration, the following services are provisioned:

- Service 1: IES providing Internet access. This service requires a CIR of 10 Mb/s and a PIR of 100 Mb/s.
- Service 2: VLL service providing FTP connectivity between Site A and Site B. This service requires a CIR of 10 Mb/s and a PIR of 20 Mb/s.
- Service 3: VPLS for video conferencing over sites A, B, and C. This service requires a CIR of 20 Mb/s and a PIR of 50 Mb/s.
- Service 4: VPLS for voice traffic. This service 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 above configuration with rate limiting using HQoS at Site A. Note that similar steps would be necessary to configure HQoS for Subscriber 1 on sites B and C:

- configure a scheduler policy
- create Subscriber 1
- create the aggregation scheduler for Subscriber 1 site A and assign ingress and egress scheduler policies to the aggregation scheduler.
- Create VLL, VPLS, and IES services for Subscriber 1. During service creation:
 - 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 will be commonly 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 values specified in the queue.

If one of the access interfaces did not participate in the scheduler aggregator, it could be governed by a separate scheduler policy.

23 — VLL service management

- 23.1 VLL service management overview 23-2**
- 23.2 Sample VLL service 23-4**
- 23.3 Workflow to create a VLL service 23-6**
- 23.4 VLL service management menus 23-6**
- 23.5 VLL service management procedures list 23-7**
- 23.6 VLL service management procedures 23-7**

23.1 VLL service management overview

The 5620 SAM supports the provisioning of Layer 2 VLL services on edge 7750 SRs. A VLL is a pipe that connects access interfaces. A VLL that connects access interfaces on one device (or site) is called a local VLL service. A VLL that connects access interfaces on two devices (or sites) is called a distributed VLL service.

For the distributed VLL service, subscriber data enters the service through two access interfaces on different edge 7750 SRs. The VLL is transported across an IP and/or IP/MPLS provider core network in circuits that are carried by service tunnels. Service tunnels are created using GRE or MPLS LSPs.

A new or existing VLL can be configured as the spoke of an HVPLS. See “HVPLS” in section 24.1 for more information.

When you configure or modify a service, you can:

- configure, modify, and specify access interfaces for the service
- associate previously created service tunnels with circuits, or configure the 5620 SAM to automatically create and associate service tunnels with circuits

Packets that arrive at an edge 7750 SR are associated with a VLL service based on the access interface on which they arrive. An access interface is uniquely identified by the:

- physical Ethernet port or POS port and channel
- encapsulation type
- encapsulation identifier (if required)

The 5620 SAM supports end-to-end VLL service configuration using a sequence of configuration forms and steps. To create a service, choose a subscriber from the Service Management→Manage Subscribers/Services form and configure a service for the chosen subscriber. Figure 23-1 shows the Create Service form with the Define Service Type parameters displayed and with VLL chosen as the service type.

Figure 23-1 VLL Create Service - Define Service Type form

Define Service Type

Service ID: Auto-Assign ID

Service Name:

Description:

Type:

Layer 2 access interfaces can be configured and specified for the service during service configuration. Figure 23-2 shows the Create L2 Interface creation form with the Select Site parameters that appears when you choose to add access interfaces to the service from the main service creation form.

Figure 23-2 VLL Create L2 Interface - Select Site form

Steps

1. Select Site
2. Select Port
3. Define General Properties
4. Select QoS Policies
5. Aggregation
6. Select Ingress and Egress Scheduler Policies
7. Select ACL Filters
8. Select Accounting Policy

Select Site

Sites In This Service:

Site ID	Site Name

Site ID: Site Name:

Common to all 7750 SR 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 7750 SR services:

- QoS policies to defines 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.
- Scheduling policies to define hierarchical rate limiting and scheduling to govern the scheduling of queues. Scheduler policies are configured using the Scheduler Policy Manager.
- 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.

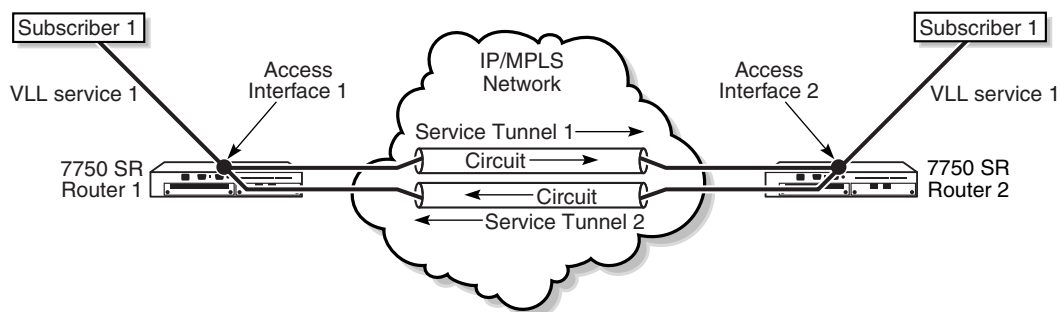
See chapter 20 for more information about policies.

OAM diagnostics can be performed on per-service basis. See chapter 29 for more information.

23.2 Sample VLL service

Figure 23-3 shows a sample VLL service.

Figure 23-3 Sample VLL service



17237

Assuming the core IP/MPLS network and service tunnels have already been configured, the following high-level tasks are required to configure this sample VLL service.

Table 23-1 Sample VLL service configuration

Task	Description
1. Configure policies as required	<p>Policies should be configured prior to creating a service. Participation in policies is defined when you configure or modify resources such as access interfaces or circuits VLL during service creation or modification. The following key policies can be applied to resources that are part of a VLL service.</p> <ul style="list-style-type: none"> • Access ingress and egress interface policies. Choose Policies→Access Ingress Policy or Policies→Access Egress Policy to open these forms. • Scheduler policy. Choose Policies→Scheduler Policy Manager to open the scheduler policy form. • ACL IP and MAC filter policies. Choose Policies→Scheduler Policy Manager to open the scheduler policy form. • Accounting policy. Choose Policies→Accounting Policy to open the accounting policy form.
2. Configure ports as access ports for use in the service	<p>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.</p>
3. Configure service tunnels as required	<p>Choose Topology→Service Tunnel Manager to create service tunnels. Service tunnels carry service traffic between edge managed devices by circuits aggregated in unidirectional service tunnels. Circuits can be associated with service tunnels during service configuration.</p> <p>During service creation, you can also configure the 5620 SAM to automatically create and associate service tunnels with circuits. In this case, you do not have to create service tunnels before you create the service.</p>
4. Create and configure Subscriber 1	<p>Choose Service Management→Manage Subscribers/Services to open the subscriber manager form and create a subscriber.</p>
5. Create and configure Service 1	<p>Click on the Services tab on the subscriber manager form and click on the Add button to create a new service. A series of steps, substeps, and forms guide the user through the service creation process. You configure the following key elements when you configure Service 1.</p> <ul style="list-style-type: none"> • Define the service type as VLL. • Specify Router 1 and Router 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: <ul style="list-style-type: none"> • Specify the routers (sites). • Specify the ports for the access interfaces. Ports must be configured as access ports. • Specify participation of access interfaces in access ingress and egress policies as required. • Specify if the access interfaces will participate in aggregation rate limiting across a card or port. If aggregation is not required, specify the participation of access interfaces in ingress and egress scheduler policies. If aggregation is required, specify the participation of access interfaces in an aggregation scheduler policy. • Specify participation of access interfaces in scheduler policies as required. <p>Create and configure circuits in both directions. Associate the circuit going from Router 1 to Router 2 with Service Tunnel 1. Associate the circuit going from Router 2 to Router 1 with Service Tunnel 2. You can also configure the 5620 SAM to automatically create and associate service tunnels with circuits.</p>
6. Create access spoke circuits for subscribers	<p>Click on the Circuits tab on the subscriber form and click on the Add Spoke button to create an HVPLS access spoke using a new or existing VLL. A series of steps, substeps, and forms guide the user through the access spoke creation process. You configure the following key elements when you configure access spokes.</p> <ul style="list-style-type: none"> • Specify the subscriber. • Select the source as a new or existing VLL or VPLS service. • When a new service is created, create a VPLS or VLL service and configure the access interfaces. • Select the source site ID for the access spoke circuit. • Select the destination of the access spoke circuit, either a new or existing service, or a site. • Specify existing service tunnels and a VC ID for the access spoke circuit as required. • Specify the spanning tree protocol on the access spoke circuit as required.

23.3 Workflow to create a VLL service

- 1 Set up group and user access privileges.
- 2 Configure the network:
 - i Build the IP or IP/MPLS core network.
 - ii Configure ports for the service as access ports.
 - iii Configure service tunnels if required.
- 3 Configure pre-defined QoS, scheduling, filter, and accounting policies.
- 4 Provision the service:
 - i Set up subscribers or associate existing subscribers with the new service.
 - ii Create the VLL service.
 - Define the service type as VLL
 - Ensure that the LSP network is configured when the transport mechanism is MPLS
 - Specify the devices (sites) used in the service
 - Specify the access interfaces
 - Specify aggregation on a service basis, or across a card or port
 - Specify QoS, scheduling, accounting, and filter policies
- 5 Create circuits to use the service tunnels.
- 6 Turn up the service.
- 7 Add spoke access circuits for HVPLS, as required.

23.4 VLL service management menus

Table 23-2 lists and describes the 5620 SAM service management menus.

Table 23-2 VLL service management menus

Menu item	Description
Service Management→Manage Subscribers/Services	Create subscribers, add or create services, and add access spoke circuits for HVPLS.
Service Management→Create Service	Create a service
Service Management→Browse Services	Perform a filtered search on services
Topology→Service Path Topology	View a graphical representation of SDPs

23.5 VLL service management procedures list

Table 23-3 lists the procedures necessary to perform VLL service management tasks.

Table 23-3 5620 SAM VLL service management procedures list

Procedure	Purpose
To create a VLL service	Create a VLL service.
To modify a VLL service	Modify a VLL service.
To add access spoke circuits for an HVPLS	Add access spoke circuits to connect sites into a new or existing VPLS mesh, which creates an HVPLS
To delete a VLL service	Delete a VLL service.
To view the service topology	View a graphical representation of VLL services that shows the sites and interfaces.

23.6 VLL service management procedures

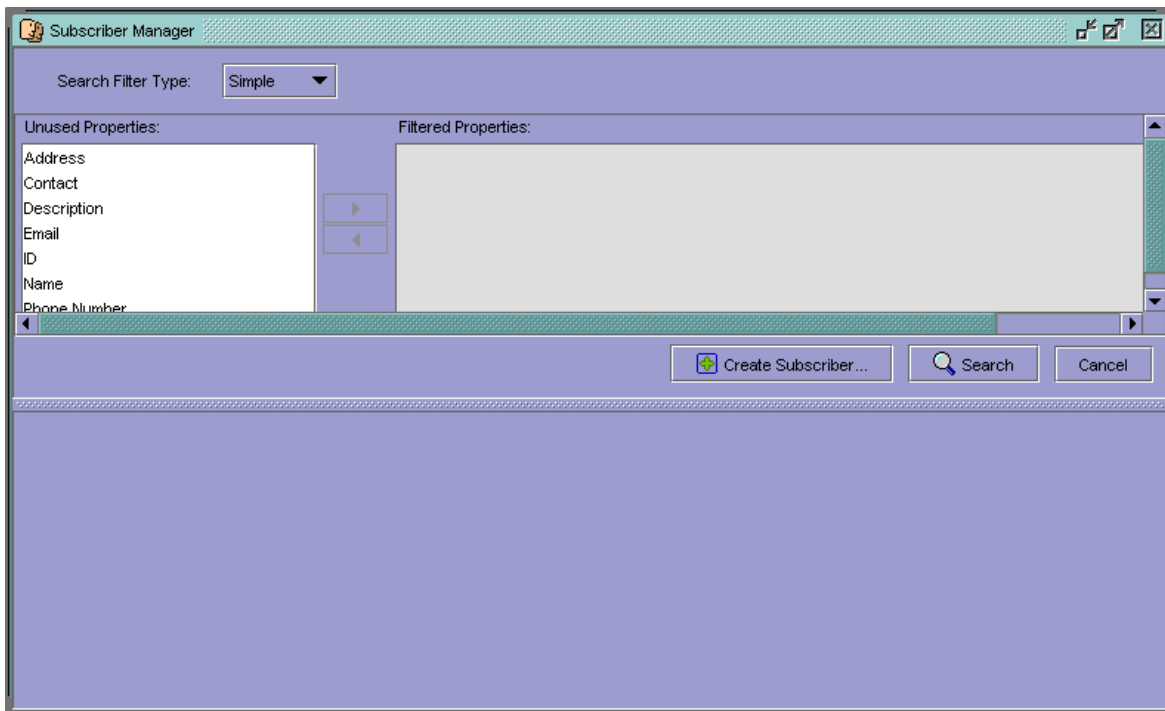
Use the following procedures to perform VLL creation and management tasks. See the *7750 SR OS Services Guide* for more information about VLL configuration and parameters.

Procedure 23-1 To create a VLL service

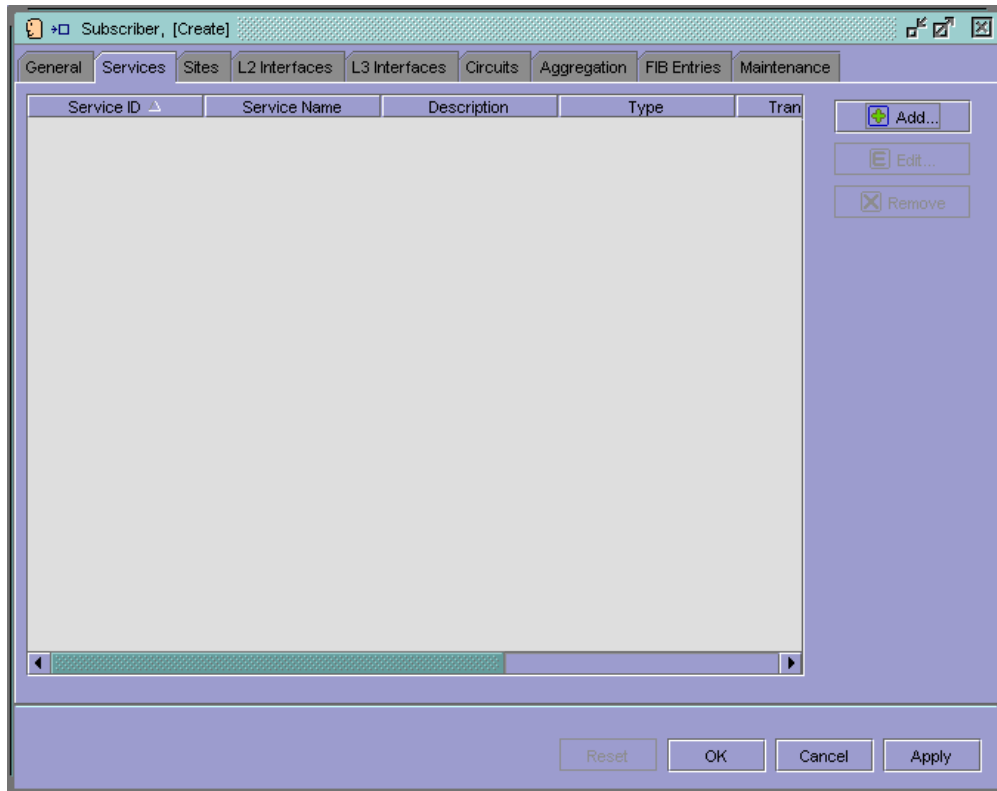
This procedure describes how to create a VLL service using the Subscriber Manager form as the starting point. This allows you to browse a list of subscribers, and choose a subscriber for the service before you start creating the service.

You can also create a VLL service using the Create Service form as the starting point. This allows you to choose a subscriber for the service during service configuration. Choose Service Management→Create Service from the 5620 SAM main menu.

- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu. The Subscriber Manager form opens as shown in Figure 23-4.

Figure 23-4 Subscriber Manager form

- 2 Configure the subscriber list filter parameters and click on the Search button. A list of available subscribers appears at the bottom of the Subscriber Manager form.
- 3 Choose a subscriber from the list to use the VLL service you are creating.
- 4 Click on the Edit button. The Subscriber form with the General tab opens.
- 5 Click on the Services tab. Figure 23-5 shows the Subscriber form with the Services tab selected.

Figure 23-5 Subscriber form — Services

- 6 Click on the Add button. The Create Service - Define Service Type form opens, with VPLS chosen as the default service type, as shown in Figure 23-6.

Figure 23-6 Create Service - Define Service Type form

The screenshot shows a web-based form titled "Create Service - Define Service Type". On the left is a "Steps" sidebar with six items, the first of which is highlighted. The main content area is titled "Define Service Type" and contains the following fields:

- Service ID:** A text input field containing the number "0". To its right is a checked checkbox labeled "Auto-Assign ID".
- Service Name:** An empty text input field.
- Description:** An empty text input field.
- Type:** A dropdown menu currently showing "VPLS".

At the bottom of the form are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Configure the parameters.

- i Specify how you want service IDs assigned. The ID uniquely identifies the service in the service domain.
 - To have the 5620 SAM automatically assign a service ID, select the Auto-Assign ID check box.
 - To manually assign a service ID, deselect the Auto-Assign ID check box. Configure the Service ID parameter. The range is 1 to 2 147 483 647
 - ii Configure the Service Name parameter. The name can be up to 32 characters.
 - iii Configure the service Description parameter. The description can be up to 80 characters.
 - iv Choose VLL for the Type parameter.
- 7 Click on the Next button. The Create Service - Configure Transport Preferences form opens, as shown in Figure 23-7.

Figure 23-7 Create Service - Configure Transport Preferences form

Configure the parameters.

- i Configure the Topology Auto-Completion parameter. The options are Manual: User Defined Connectivity, and All Access Sites Fully Meshed (No Hierarchy).

When you choose Manual: User Defined Connectivity, you must create circuits for the service and bind the circuits to a service tunnel in step 25 of this procedure.

When you choose All Access Sites Fully Meshed (No Hierarchy), circuits for the service are automatically created and bound to service tunnels.

- ii When you choose All Access Sites Fully Meshed (No Hierarchy), configure the Transport Type parameter. The options are Any, GRE, or MPLS:RSVP-LSP.



Note — To use MPLS as the transport type, you must bind LSPs to service tunnels during service tunnel configuration. See Procedure 19-1 for more information.

- iii When you choose All Access Sites Fully Meshed (No Hierarchy), configure the Use Bandwidth- Reserved Paths parameter. The options are No Preference, Never, or Always.

8 Click on the Next button. The Create Service - Configure Sites form opens.

9 Click on the Add button. The Create Service Site - Number of Sites form opens, as shown in Figure 23-8.

Figure 23-8 Create Service Site - Number of Sites form

Choose Single from the drop-down menu to add and configure a single site. After you configure the site, you can add and configure additional sites.



Note — You can add and configure multiple sites at the same time. Choose Multiple from the drop-down menu and follow the series of steps that appears.

- 10 Click on the Next button. The Create Service Site - Select Site form opens.
Click on the Select button to list and choose a site.
- 11 Click on the Next button. The Create Service Site - Define General Properties form opens.
Configure the parameters.
 - i Configure the Description parameter. The description can be up to 80 characters.
 - ii Configure the site Administrative State parameter. The options are Up or Down.
- 12 Click on the Next button. The Create Service Site - Define MTU form opens.
Configure the MTU parameter. The range is 0 to 9194.
- 13 Click on the Next button. The Create Service Site - Configure L2 Interfaces form opens, as shown in Figure 23-9.

Figure 23-9 Create Service Site - Configure L2 Interfaces form

Steps

1. Number of Sites
2. Select Site
3. Define General Properties
4. Define MTU
5. Configure L2 Interfaces

Configure L2 Interfaces

Site ID	Site Name	Service ID	Service Name

Buttons: Add..., Edit..., Remove

Bottom Buttons: < Back, Next >, Finish, Cancel

- 14 Click on the Add button. The Create L2 Interface - Select Port form opens, as shown in Figure 23-10.

Figure 23-10 Create L2 Interface - Select Port form

Steps

1. Select Port
2. Define General Properties
3. Aggregation
4. Select Ingress and Egress Scheduler Policies
5. Select ACL Filters

Select Port

Port:

Port ID:

Encap Type:

Outer Encapsulation Value: Inner Encapsulation Value:

Bottom Buttons: < Back, Next >, Finish, Cancel

Configure the parameters.

- i Click on the Select button to list and choose a port or channel.

You can only choose ports or channels in access mode. Use the 5620 SAM navigation tree to choose a port or channel and set the Mode parameter to Access.

After you choose a port or channel, additional steps to configure the interface appear, as shown in Figure 23-11.

Figure 23-11 Create L2 Interface - Select Port form

- ii Configure the Inner Encapsulation Value and the Outer Encapsulation Value parameters.

One or both parameters are configurable when the port encapsulation type is Dot1q, Q in Q, BCP Dot 1q, or FR. Use the 5620 SAM navigation tree to choose a port or channel and specify an option for the port Encap Type parameter.

The range for the Inner Encapsulation Value and the Outer Encapsulation Value parameters depend on the option you choose for the port Encap Type parameter.

- 15 Click on the Next button. The Create L2 Interface - Define General Properties form opens.

Configure the parameters.

- i Configure the interface Description parameter. The description can be up to 80 characters.
 - ii Configure the interface Administrative State parameter. The options are Up or Down.
- 16** Click on the Next button. The Create L2 Interface - Select QoS Policies form opens, as shown in Figure 23-12.

Figure 23-12 Create L2 Interface - Select QoS Policies

- i Click on the Ingress: Select button to list and choose an access ingress policy.
 - ii Click on the Egress: Select button to list and choose an access egress policy.
- 17** Click on the Next button. The Create L2 Interface - Aggregation form opens.

Configure the Aggregation parameter. The parameter specifies whether an aggregation scheduler policy will be applied to the interface. The option are On or Off.

When you choose On, go to step 18 of this procedure.

When you choose Off, go to step 19 of this procedure.

- 18** Click on the Next button. The Create L2 Interface - Select Aggregation Scheduler Policy form opens.

Click on the Select button to list and choose an aggregation scheduler policy.

Go to step 20 of this procedure.

- 19** Click on the Next button. The Create L2 Interface - Select Ingress and Egress Scheduler Policies form opens.
 - i** Click on the Ingress: Select button to list and choose an ingress scheduler policy.
 - ii** Click on the Egress: Select button to list and choose an egress scheduler policy.
- 20** Click on the Next button. The Create L2 Interface - Select ACL Filters form opens.
 - i** Click on the Ingress: Select button to list and choose an ingress ACL filter.
 - ii** Click on the Egress: Select button to list and choose an egress ACL filter.
- 21** Click on the Next button. The Create L2 Interface - Select Accounting Policy form opens.

Configure the parameters.

 - i** Click on the Select button to list and choose an accounting policy.
 - ii** Select the Accounting Enabled check box to enable the collection of accounting statistics for the interface.
- 22** Click on the Finish button. The the Create L2 Interface - Select Accounting Policy form closes and the Create Service Site - Configure L2 Interfaces form re-opens. The interface and interface parameters are listed.

You can add, edit, or remove interfaces.
- 23** Click on the Finish button. The Create Service Site - Configure L2 Interfaces form closes and the Create Service - Configure Sites form re-opens. The site and the site parameters are listed.

You can add, edit, or remove sites.
- 24** Click on the Next button. The Create Service - L2 Interfaces Summary form opens as shown in Figure 23-13.

Figure 23-13 Create Service - L2 Interfaces Summary form

Steps

1. Define Service Type
2. Configure Transport Preferences
3. Configure Sites
4. L2 Interfaces Summary
5. Circuits Summary

L2 Interfaces Summary
You may add/edit/remove interfaces

Site ID	Site Name	Service ID	Service Name
10.1.1.18		0	

Buttons: Add..., Edit..., Remove

Navigation: < Back, Next >, Finish, Cancel

Interface and interface parameters are listed. You can add, edit, or remove interfaces.

- 25 Click on the Next button.
 - a If you chose Manual: User Defined Connectivity in step 7 of this procedure, the Create Service - Configure Circuits form opens. Go to step 26 of this procedure.
 - b If you chose All Access Sites Fully Meshed (No Hierarchy) in step 7 of this procedure, the Circuits Summary form opens. Circuits are automatically created and associated with the service. Go to step 34 of this procedure.
- 26 In the Create Service - Configure Circuits form, click on the Add button. The Create Circuit - Select Source Node form opens, as shown in Figure 23-14. Choose a source node.

Figure 23-14 Create Circuit - Select Source Node form

Site ID ▾	Site Name	Description	Admin
38.120.182.21	138.120.182.21		Up
38.120.182.23	138.120.182.23		Up

Source Node ID: Source Node Name:

< Back Next > Finish Cancel

- 27 Click on the Next button. The Create Circuit - Select Destination Node form opens.
 - a If the destination node is a managed site, choose a site from the list.
 - b If the destination node is an unmanaged site, specify the system ID for the Destination Node ID parameter.
- 28 Click on the Next button. The Create Circuit - Select Tunnel form opens. Configure the parameters.
 - a If you want to manually specify a tunnel to be bound to the circuit, click on the Select button to list and choose a tunnel.
 - b If you want the 5620 SAM to automatically select a tunnel to be bound to the circuit, or create and bind a service tunnel to the circuit:
 - i Configure the Tunnel Transport parameter for the outgoing tunnel. The 5620 SAM will choose an existing tunnel based on the transport type, or create a new tunnel if one does not exist. The 5620 SAM will automatically bind the tunnel to the circuit you are creating.
 - ii Configure the Tunnel Transport parameter for the return tunnel. The 5620 SAM will choose an existing tunnel based on the transport type, or create a new tunnel if one does not exist. The 5620 SAM will automatically bind the return tunnel to the return circuit.
- 29 Click on the Next button. The Create Circuit - Define General Properties form opens. Configure the circuit Administrative State parameter. The options are Up or Down.
- 30 Click on the Next button. The Create Circuit - Define VC Properties form opens.

Configure the parameters.

- i Configure the VC Type parameter. The parameter specifies the default VC type signaled for the circuit to service tunnel binding to the far end of a spoke service tunnel. The actual signaling of the VC type depends on the signaling parameter defined for the service tunnel. The options are Ethernet, VPLS, or VLAN.
 - ii Configure the VLAN VC Tag parameter. The parameter specifies an explicit dot1q value for encapsulation to far end of the service tunnel. The range is 0 to 4094.
- 31** Click on the Next button. The Create Circuit - Select ACL Filters form opens.
- i Click on the Ingress: Select button to list and choose an ingress ACL filter.
 - ii Click on the Egress: Select button to list and choose an egress ACL filter.
- 32** Click on the Finish button. The Create Circuit - Select ACL Filters form closes and the Create Service - Configure Circuits form re-opens.

You can list the circuits and view circuit parameters in the circuit list that appears at the bottom of the form. Choose the Unidirectional or Bidirectional parameter and selecting devices from the To and/or From lists. The circuits that appear in the circuits list are filtered according to the criteria you specify.

You can add, edit, or remove circuits.



Note — For a distributed VLL service, you must create circuits in both directions. For a local VLL service, circuits are not required.

- 33** Click on the Next button. The Create Service - Circuits Summary form opens. Circuits and circuit parameters are listed in the form.

You can add, edit, or remove circuits. To edit circuits:

- i Select a circuit from the list.
- ii Click on the Edit button.

The Circuit (Create) properties form with the General tab opens.

- iii Click on a tab and configure the parameters as required. The parameters include:
 - Type parameter to specify the type of circuit. The options are Spoke or Mesh.
 - Tunnel ID parameter
 - VLAN VC Tag parameter
- iv Close the form.

The modified parameters for the circuit appear in the list.

- 34 Click on the Finish button. The Create Service - Circuits Summary form closes and the Subscriber Manager form re-opens. The service and service parameters are listed in the form.

You can add, edit or remove services.

- 35 Click on the Apply button to save the service.
-

Procedure 23-2 To modify a VLL service

- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu.
- 2 Configure the subscriber list filter parameters and click on the Search button. A list of available subscribers appears at the bottom of the Subscriber Manager form.
- 3 Choose a subscriber from the list.
- 4 Click on the Edit button. The Subscriber form with the General tab opens.
- 5 Click on the Services tab. A list of services appears.
- 6 Choose a service.
- 7 Click on the Edit button. A Service edit form with the General tab opens.
- 8 Modify the parameters for the service as required.



Caution — Modifying parameters can be service-affecting.

The parameter information that appears for the service includes:

- General tab that displays the general properties of the service
 - Transport tab that displays the transport information for the service
 - Sites tab that lists the sites included in the service
 - L2 Interface tab that lists interfaces used by the service
 - Circuits tab that lists circuits used by the service
 - Maintenance tab that lists OAM diagnostics that can be performed to diagnose the service
 - Faults tab that displays faults associated with the service
- 9 Click on the OK button to close the Service edit form. The Subscriber form re-opens.
 - 10 Click on the Apply button to save the modified service.
-

Procedure 23-3 To add access spoke circuits for an HVPLS

See Procedure 24-4 in chapter 24 to create the spoke for the HVPLS using a new or an existing VLL. During the procedure, choose the VLL-related options. For more information about the parameters and procedures to create a VLL, see Procedure 23-1 in this section.

Procedure 23-4 To delete a VLL service

- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu.
 - 2 Configure the subscriber list filter parameters and click on the Search button. A list of available subscribers appears at the bottom of the Subscriber Manager form.
 - 3 Choose a subscriber from the list.
 - 4 Click on the Edit button. The Subscriber form with the General tab opens.
 - 5 Click on the Services tab. A list of services appears.
 - 6 Choose a service.
 - 7 Click on the Remove button. The service is removed from the list.
 - 8 Click on the Apply button to delete the service.
-

Procedure 23-5 To view the service topology

- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu.
 - 2 Configure the subscriber list filter parameters and click on the Search button. A list of available subscribers appears at the bottom of the Subscriber Manager form.
 - 3 Choose a subscriber from the list.
 - 4 Click on the Edit button. The Subscriber form with the General tab opens.
 - 5 Click on the Services tab. A list of services appears.
 - 6 Choose a service.
 - 7 Click on the Edit button. A Service edit form with the General tab opens.
 - 8 Click on the Topology view button. The service topology map opens.
-

24 — VPLS management

- 24.1 VPLS management overview 24-2**
- 24.2 Sample VPLS configuration 24-7**
- 24.3 Workflow to create a VPLS 24-13**
- 24.4 VPLS management menus 24-14**
- 24.5 VPLS management procedures list 24-14**
- 24.6 VPLS management procedures 24-14**

24.1 VPLS management overview

The 5620 SAM supports VPLS multipoint switched service on edge 7750 SRs and 7450 ESSs. 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. Customers sites in the VPLS appear to be on the same LAN, even if the sites are geographically dispersed.

The advantages of VPLS include:

- Uses an Ethernet interface on the customer access side to simplify provisioning.
- Enables customers to control and simplify routing strategies, as all routers in the VPLS are part of the same LAN, which simplifies IP addressing.
- VPLS is protocol independent, which means there is no Layer 2 protocol conversion between LAN and WAN technologies.

VPLS can span a single or multiple sites. A VPLS that spans a single site is called a local VPLS. In a local VPLS, subscriber 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.

When you configure or modify a service, you can:

- configure, modify, and specify access interfaces for the service
- associate previously created service tunnels with circuits, or configure the 5620 SAM to automatically create and associate service tunnels with circuits

Packets that arrive at an edge device are associated with an VPLS based on the access interface on which they arrived. An access interface is uniquely identified by the:

- physical Ethernet port or POS port and channel
- encapsulation type
- encapsulation identifier (if required)

The 5620 SAM supports end-to-end VPLS configuration using a sequence of configuration forms and steps. To create a service, choose a subscriber from the Service Management→Manage Subscribers/Services form and configure a service for the chosen subscriber. Figure 24-1 shows the Create Service form with the Define Service Type parameters displayed and VPLS chosen as the service type.

Figure 24-1 VPLS main service creation - Define Service Type form

Steps

1. Define Service Type
2. Configure Transport Preferences
3. Configure Sites
4. L2 Interfaces Summary
5. Configure Circuits
6. Circuits Summary

Define Service Type

Service ID: Auto-Assign ID

Service Name:

Description:

Type:

< Back Next > Finish Cancel

Layer 2 access interfaces can be configured and specified for the service during service configuration. Figure 24-2 shows the Create L2 Interface creation form with the Select Site parameters displayed. The form opens when you choose to add access interfaces to the service from the main service creation form.

Figure 24-2 VPLS Create L2 Interface - Select Site form

Steps

1. Select Site
2. Select Port
3. Define General Properties
4. Select QoS Policies
5. Aggregation
6. Select Ingress and Egress Scheduler Policies
7. Select ACL Filters
8. Select Accounting Policy
9. Configure Spanning Tree Protocol

Select Site

Sites In This Service:

Site ID	Site Name	
10.1.1.23	pc23	1500
10.1.1.30	pc30	1500

Edit...
Select Other...

Site ID: Site Name:

< Back Next > Finish Cancel

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.
- Scheduling policies to define hierarchical rate limiting and scheduling to govern the scheduling of queues. Scheduler policies are configured using the Scheduler Policy Manager.
- 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.

See chapter 20 for more information about policies.

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 29 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 VPLSs 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
- 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

HVPLS

A hierarchical VPLS is created by enhancing the VPLS core mesh with access spoke circuits interconnected to another VPLS, a VLL, or a site.

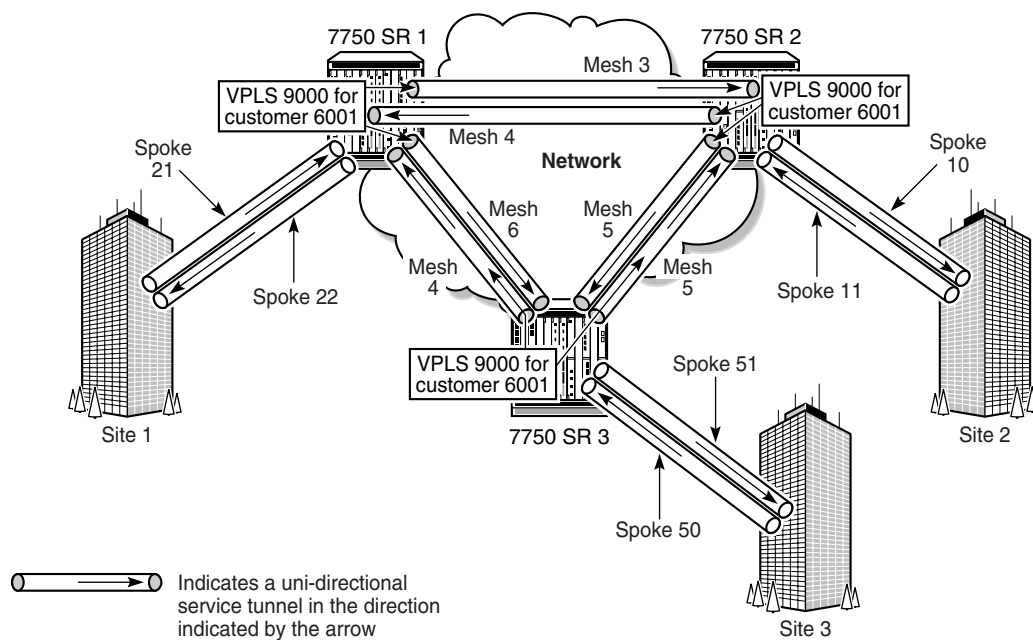
HVPLS can:

- reduce the complexity of mesh configuration
- decrease the amount of signaling of routes between devices

When traffic arrives at an access spoke circuit, it acts equivalently to a bridge port, where flooded traffic received on the access spoke is replicated to all other spokes, meshes, or service access points but is not transmitted on the port where it is received.

Figure 24-3 shows a sample HVPLS with a mesh and spoke configuration. For example, spokes 50 and 51 are uni-directional access spoke circuits bound to service tunnels. The access spoke circuits exist within the context of a VLL or VPLS service which is interconnected to the original, fully meshed VPLS. Alternately, the access spoke circuit can provide interconnectivity to a service site.

Figure 24-3 HVPLS configuration



17438

The 5620 SAM supports the following HVPLS interconnectivity via access spoke circuits:

- VPLS to VPLS
- VPLS to VLL
- VPLS to service site

FIBs

The edge devices perform the packet replication required for broadcast and multicast traffic across the bridged domain. MAC address learning is performed 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 routers 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 a Layer 2 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 ingresses on a SAP. A remote MAC address is a MAC address received via 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.

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

Alcatel STP incorporates STP parameters with some modifications to make the operational characteristics of VPLSs more effective. This version(s) of the protocol that are supported depends on the type of device.

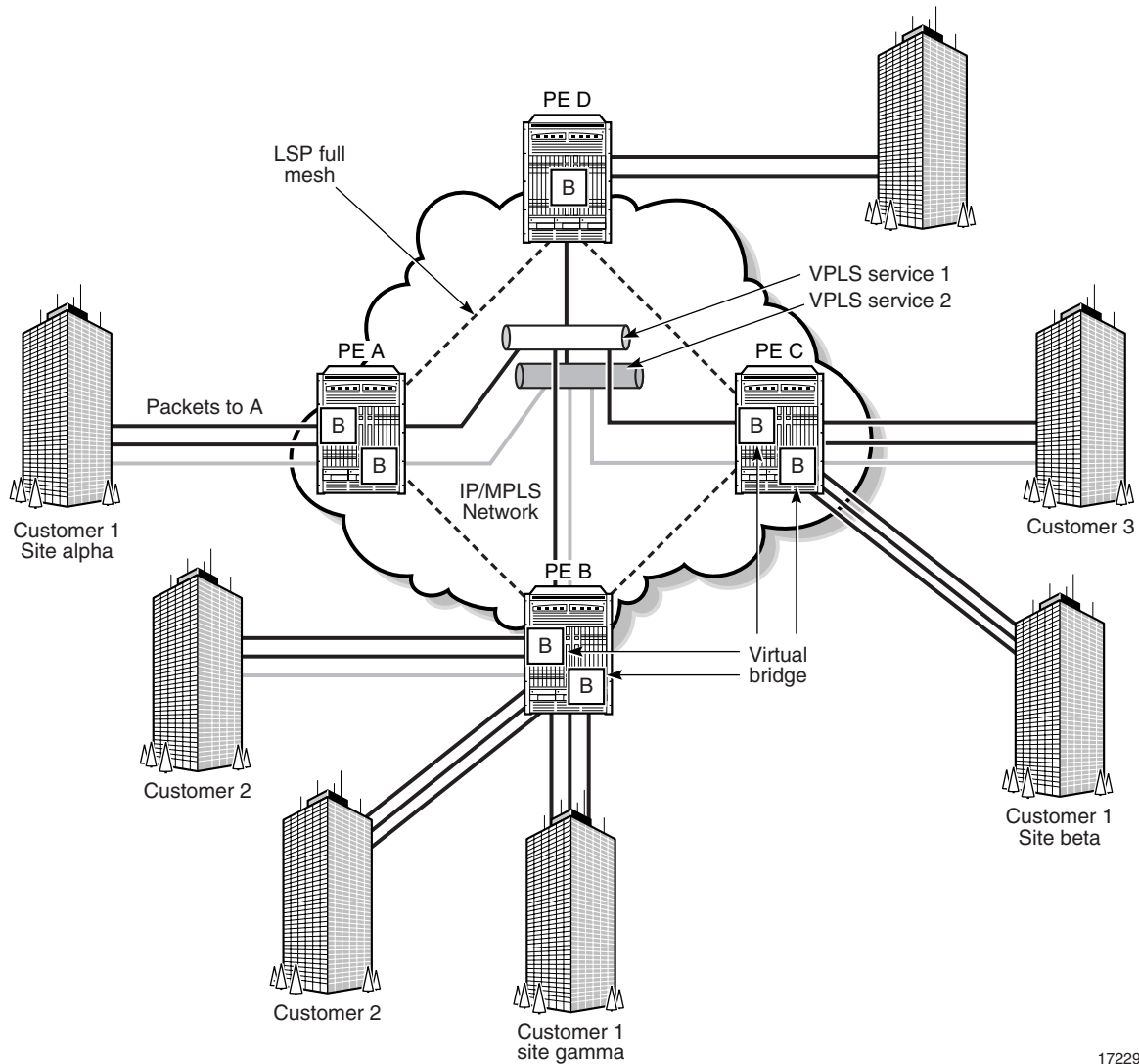
For example, 7750 SRs use an optimized and compatible implementation of IEEE 802.1D STP, which attempts to eliminate STP blocking of links within the core of the VPLS, the core network. The parameters you set allow the balancing of resiliency and speed of convergence extremes.

The 7450 ESS can use multiple spanning tree protocols in addition to IEEE 802.1D, for example, 802.1w. STP on the 7450 ESS in order to guarantee that service tunnels will not be blocked in any circumstance without imposing artificial restrictions on the placement of the root bridge within the network. The modifications introduced are fully compliant with the 802.1D STP specification. In order to achieve this, all mesh service tunnels are configured as either root ports or designated ports using the appropriate parameters.

24.2 Sample VPLS configuration

Figure 24-4 shows a sample VPLS configuration.

Figure 24-4 Sample VPLS



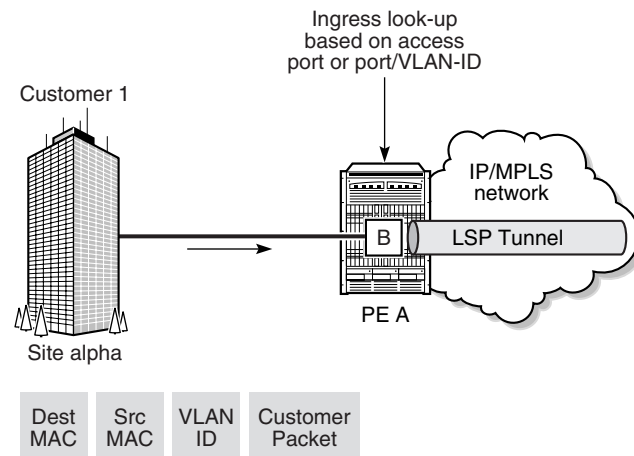
17229

VPLS service 1 is a distributed service, consisting of customer 1 connected to PE A, customer 2 connected to PE B, and customer 3 connected to PE C. All three customers belong to VPLS service 1.

In the following example, Customer 1 wants to send data from site alpha to site beta. Although the following examples do not display this, customer 2 has a local service.

Customer 1 packets arriving at PE A are associated to the appropriate VPLS service 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 24-5.

Figure 24-5 Packet forwarding by ingress router PE A

17230

The MAC address can be:

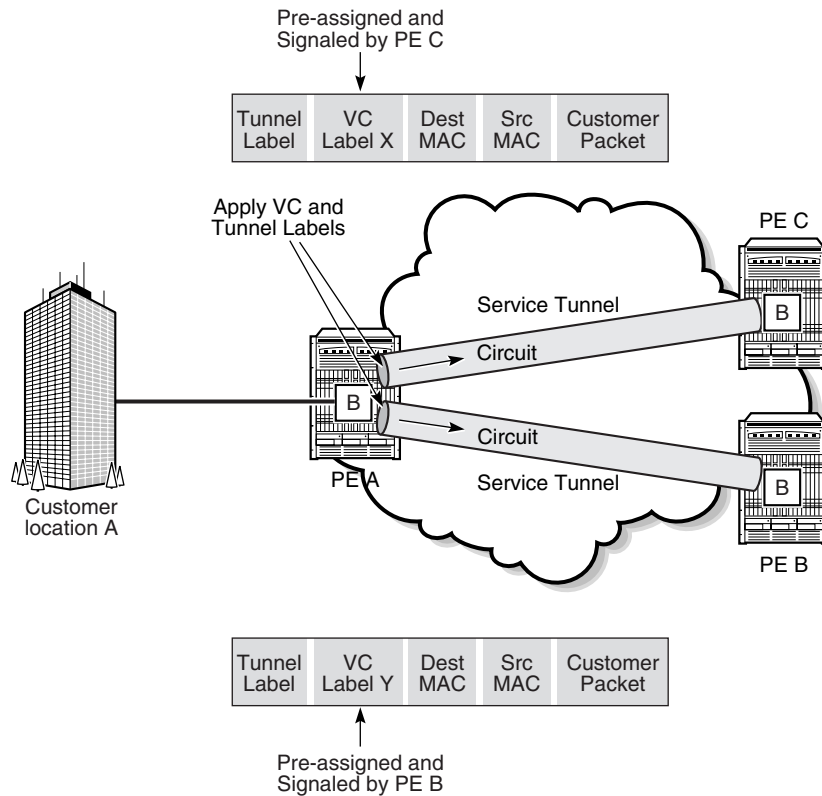
- known
- unknown

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 once the VC label is removed and the transport label is added to the packet, as shown in Figure 24-5.

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 service 1. PE A uses the VC labels (VLAN IDs) that PE B and PE C previously signaled for this VPLS service 1.

As shown in Figure 24-6, the packets from PE A are transported across the core IP/MPLS network.

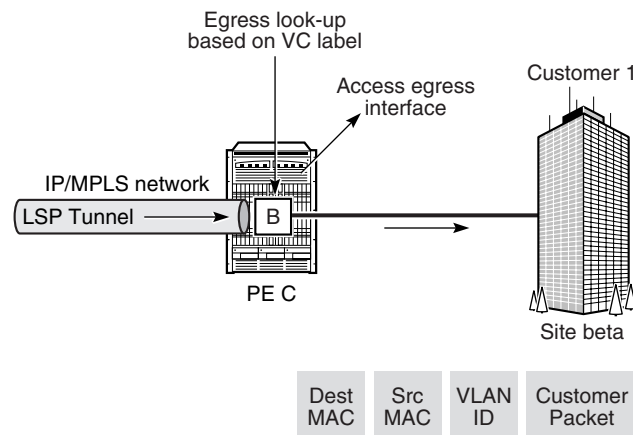
Figure 24-6 Packet forwarding from PE A across the core IP/MPLS network



17231

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 takes away the tunnel label to reveal the VC label that identifies that these packets belong to VPLS service 1, as shown in Figure 24-7.

Figure 24-7 Packet forwarding by the egress router PE C

17232

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. Again, the MAC address can be:

- 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 service 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 service 1.

Assuming the core IP/MPLS network and service tunnels have already been configured, the following high-level tasks are required to configure this sample VPLS.

Table 24-1 Sample VPLS configuration

Task	Description
1. Configure policies as required	<p>Policies should be configured prior to creating 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 VPLS.</p> <ul style="list-style-type: none"> • Access ingress and egress interface policies. Choose Policies→Access Ingress Policy or Policies→Access Egress Policy to open these forms. • Scheduler policy. Choose Policies→Scheduler Policy Manager 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→Acl MAC Filter Manager to open the ACL form. • Accounting policy. Choose Policies→Accounting Policy to open the accounting policy form.
2. Configure ports as access ports for use in the service	<p>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.</p>
3. Configure service tunnels as required	<p>Choose Topology→Service Tunnel Manager 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.</p> <p>During service creation, you can also configure the 5620 SAM to automatically create and associate service tunnels with circuits. In this case, you do not have to create service tunnels before you create the service.</p>
4. Create and configure Subscriber 1	<p>Choose Service Management→Manage Subscribers/Services to open the subscriber manager form and create a subscriber.</p>
5. Create and configure Service 1	<p>Click on the Services tab on the subscriber manager form and click on the Add button to create a new service. A series of steps, substeps, and forms guide the user through the service creation process. You configure the following key elements when you configure Service 1.</p> <ul style="list-style-type: none"> • Specify customer 1 as the subscriber for the VPLS. • Define the service type as VPLS. • Specify PE A, PE B, and PE C as the routers (sites) for customer 1 VPLS. • Specify the VPLS STP parameters. • Specify the VPLS FIB parameters. • Configure and specify access interfaces on each of the routers (PE A and PE C) as the access interfaces for the VPLS to site alpha and site beta. You do the following when you configure interfaces: <ul style="list-style-type: none"> • Specify the routers (sites). • Specify the ports for the access interfaces and configure the access interfaces. Ports must be configured as access ports. do • Specify participation of access interface in access ingress and egress policies as required. • Specify if the access interfaces will participate in aggregation rate limiting across a card or port. If aggregation is not required, specify the participation of access interfaces in ingress and egress scheduler policies. If aggregation is required, specify the participation of access interfaces in an aggregation scheduler policy. • Specify participation of access interfaces in a scheduler policy as required. • Create and configure circuits in both directions. • If required, associate the circuits going in both directions with tunnels going in both directions. You can also configure the 5620 SAM to automatically create and associate service tunnels with circuits

(1 of 2)

Task	Description
6. Create, update, or configure additional subscribers to the VPLS, or create a new VPLS with new or additional subscribers	Repeat the above steps as required.
7. For HVPLS, create access spoke circuits for subscribers	<p>Click on the Circuits tab on the subscriber form and click on the Add Spoke button to create an HVPLS access spoke using a new or existing VPLS or VLL service. A series of steps, substeps, and forms guide the user through the access spoke circuit creation process. You configure the following key elements when you configure access spoke circuits.</p> <ul style="list-style-type: none"> • Specify the subscriber. • Select the source as a new or existing service. • When a new service is created, create a VPLS or VLL service and configure the Layer 2 access interfaces • Select the source site ID for the access spoke circuit • Select the destination of the access spoke circuit, either an existing service or a site. • Specify existing service tunnels and a VC ID for the access spoke circuit as required. • Specify spanning tree protocol on the access spoke circuit as required.

(2 of 2)

24.3 Workflow to create a VPLS

- 1 Set up group and user access privileges.
- 2 Configure the network:
 - i Build the IP or IP/MPLS core network.
 - ii Configure ports for the service as access ports.
 - iii Configure service tunnels.
- 3 Configure pre-defined QoS, scheduling, filter, and accounting policies. You do not have to create pre-defined policies if policies are created on a per-service basis.
- 4 Provision the service:
 - i Set up subscribers or associate existing subscribers with the new service.
 - ii Create the VPLS by associating the subscriber with the VPLS. The necessary parameters are listed in Table 24-1.
 - Define the service type as VPLS.
 - Ensure the LSP network is configured when the transport mechanism is MPLS.
 - Specify the routers (sites) used in the service.
 - Specify the access interfaces.
 - Specify the STP parameters for the service as required.
 - Specify aggregation on a service basis, or across a card or port.
 - Specify QoS, scheduling, accounting, and filter policies.
 - Specify MAC ACL filters as required.
 - Configure the FIB parameters as required.

- 5 Create circuits to use the service tunnels.
- 6 Turn up the service.
- 7 Add access spoke circuits for HVPLS, as required.

24.4 VPLS management menus

Table 24-2 lists and describes the VPLS management menus.

Table 24-2 VPLS management menus

Menu item	Description
Service Management→Manage Subscribers/Services	Create subscribers, add or create services, and add access spoke circuits for HVPLS.
Service Management→Create Service	Create a service.
Service Management→Browse Services	Perform a filtered search on services.
Service Management→Manage FIB Entries or Service Management→Manage Subscribers/Services	Manage FIB entries.
Topology→Service Path Topology	View a graphical representation of SDPs.

24.5 VPLS management procedures list

Table 24-3 lists the procedures necessary to perform VPLS management tasks.

Table 24-3 VPLS management procedures list

Procedure	Purpose
To create a VPLS	Create a VPLS
To modify a VPLS	Modify a VPLS
To delete a VPLS	Delete a VPLS
To configure HVPLS using access spoke circuits	Adding access spoke circuits to connect sites into a new or existing VPLS mesh, which creates an HVPLS
To add or modify FIB entries	Manage FIB entries
To view the service topology	View a graphical representation of an VPLS that shows the sites and interfaces.

24.6 VPLS management procedures

Use the following procedures to perform VPLS creation and management tasks.

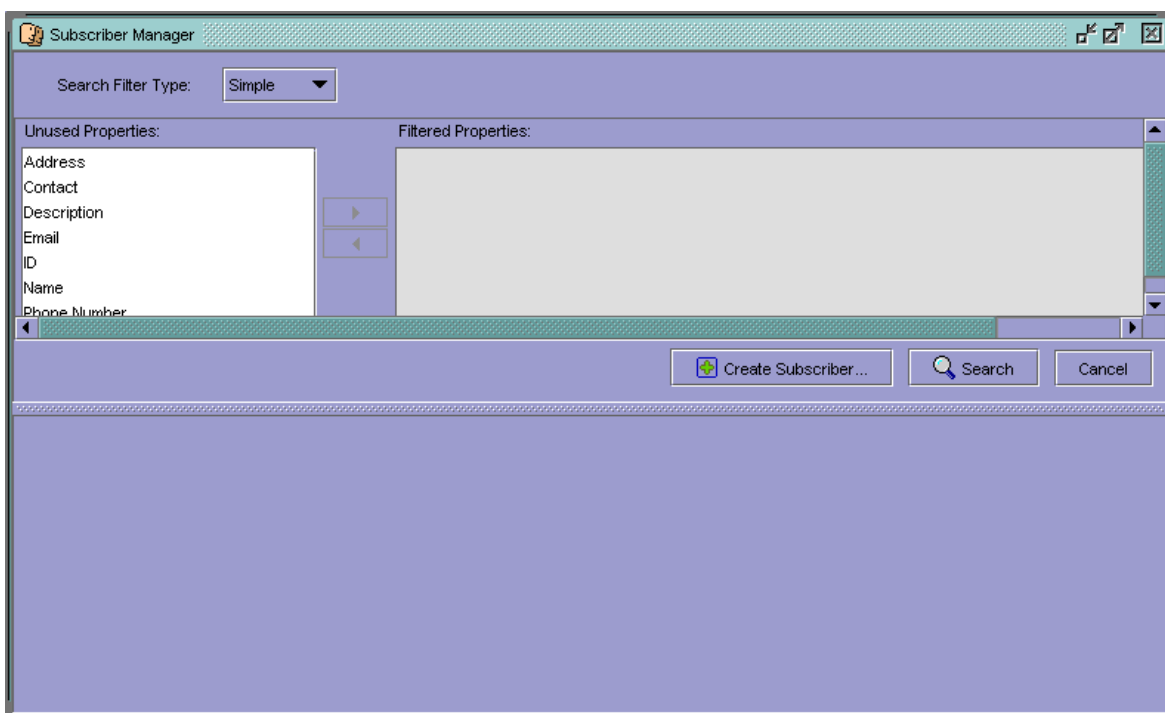
Procedure 24-1 To create a VPLS

This procedure describes how to create a VPLS using the Subscriber Manager form as the starting point. This allows you to browse a list of subscribers, and choose a subscriber for the service before you start creating the service.

You can also create a VPLS service using the Create Service form as the starting point. This allows you to choose a subscriber for the service during service configuration. Choose Service Management→Create Service from the 5620 SAM main menu.

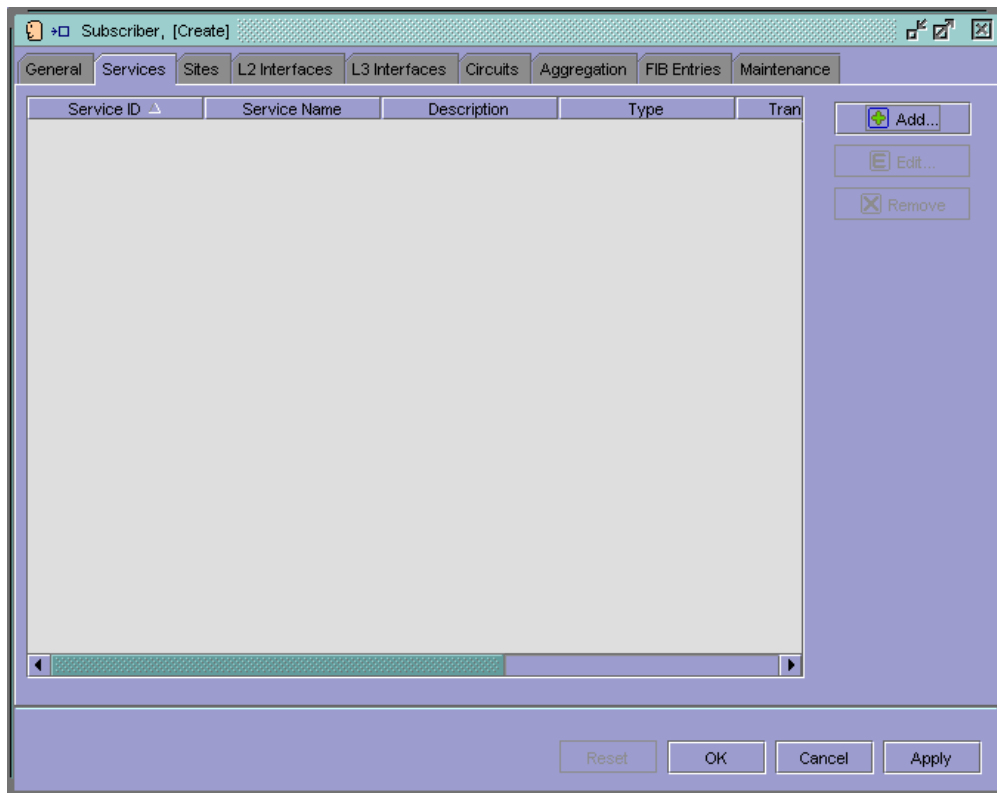
- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu. The Subscriber manager form opens as shown in Figure 24-8.

Figure 24-8 Subscriber Manager form



- 2 Configure the subscriber list filter parameters and click on the Search button. A list of available subscribers appears at the bottom of the Subscriber Manager form.
- 3 Choose a subscriber from the list to use the VPLS that you are creating.
- 4 Click on the Edit button. The Subscriber form with the General tab opens.
- 5 Click on the Services tab. Figure 24-9 shows the Subscriber form with the Services tab button selected.

Figure 24-9 Subscriber form — Services



- 6 Click on the Add button.

Click on the Add button. The Create Service - Define Service Type form opens, with VPLS chosen as the default service type, as shown in Figure 24-10.

Figure 24-10 Create service form

Configure the parameters.

- i Specify how you want service IDs assigned. The ID uniquely identifies the service in the service domain.
 - To have the 5620 SAM automatically assign a service ID, select the Auto-Assign ID check box.
 - To manually assign a service ID, deselect the Auto-Assign ID check box. Configure the Service ID parameter. The range is 1 to 2 147 483 647
 - ii Configure the Service Name parameter. The name can be up to 32 characters.
 - iii Configure the service Description parameter. The description can be up to 80 characters.
- 7 Click on the Next button. The Create Service - Configure Transport Preferences form opens, as shown in Figure 24-11.

Figure 24-11 Create Service - Configure Transport Preferences form

Configure the parameters.

- i Configure the Topology Auto-Completion parameter. The options are Manual: User Defined Connectivity, and All Access Sites Fully Meshed (No Hierarchy).

When you choose Manual: User Defined Connectivity, you must create circuits for the service and bind the circuits to service tunnels in step 29 of this procedure.

When you choose All Access Sites Fully Meshed (No Hierarchy), circuits for the service are automatically created and bound to service tunnels.

- ii When you choose All Access Sites Fully Meshed (No Hierarchy), configure the Transport Type parameter. The options are Any, GRE, or MPLS:RSVP-LSP.



Note — To use MPLS as the transport type, you must bind LSPs to service tunnels during service tunnel configuration. See Procedure 19-1 for more information.

- iii When you choose All Access Sites Fully Meshed (No Hierarchy), configure the Use Bandwidth- Reserved Paths parameter. The options are No Preference, Never, or Always.

- 8 Click on the Next button. The Create Service - Configure Sites form opens.
- 9 Click on the Add button. The Create Service Site - Number of Sites form opens, as shown in Figure 24-12.

Figure 24-12 Create Service Site - Number of Sites form

Choose Single from the drop-down menu to add and configure a single site. After you configure the site, you can add and configure additional sites.



Note — You can add and configure multiple sites at the same time. Choose Multiple from the drop-down menu and follow the series of steps that appears.

- 10 Click on the Next button. The Create Service Site - Select Site form opens.
Click on the Select button to list and choose a site.
- 11 Click on the Next button. The Create Service Site - Define General Properties form opens.
Configure the parameters.
 - i Configure the Description parameter. The description can be up to 80 characters.
 - ii Configure the site Administrative State parameter. The options are Up or Down.
 - iii Configure the Default Mesh VC ID
 - To have the 5620 SAM automatically assign a mesh VC ID, select the Auto-Assign ID check box.
 - To manually assign a mesh VC ID, deselect the Auto-Assign ID check box. Configure the Default Mesh VC ID parameter. The range is 0 to 4294967295

- 12 Click on the Next button. The Create Service Site - Define MTU form opens.
Configure the MTU parameter. The range is 0 to 9194.
- 13 Click on the Next button. The Create Service Site - Configure L2 Interfaces form opens, as shown in Figure 24-13.

Figure 24-13 Create Service Site - Configure L2 Interfaces form

The screenshot shows a web-based configuration interface. The title bar reads 'Create Service Site - Subscriber - 2'. On the left, a 'Steps' sidebar contains a list of seven steps: 1. Number of Sites, 2. Select Site, 3. Define General Properties, 4. Define MTU, 5. Configure L2 Interfaces (highlighted), 6. Configure Spanning Tree Protocol, and 7. Configure FIB. The main content area is titled 'Configure L2 Interfaces' and contains a table with four columns: 'Site ID', 'Site Name', 'Service ID', and 'Service Name'. The table is currently empty. To the right of the table are three buttons: 'Add...' (with a plus icon), 'Edit...' (with an edit icon), and 'Remove' (with a minus icon). At the bottom of the form are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

- 14 Click on the Add button. The Create L2 Interface - Select Port form opens, as shown in Figure 24-14.

Figure 24-14 Create L2 Interface - Select Port form

Configure the parameters.

- i Click on the Select button to list and choose a port or channel.

You can only choose ports or channels in access mode. Use the 5620 SAM navigation tree to choose a port or channel and set the Mode parameter to Access.

After you choose a port or channel, additional steps to configure the interface appear, as shown in Figure 24-15. The steps that appear depend on type of router on which the interface is located. For example, an additional step, Configure FIB, appears when the interface is on a 7450 ESS.

Figure 24-15 Create L2 Interface - Select Port form

- ii Configure the Inner Encapsulation Value and the Outer Encapsulation Value parameters.

One or both parameters are configurable when the port encapsulation type is Dot1q, Q in Q, BCP Dot 1q, or FR. Use the 5620 SAM navigation tree to choose a port or channel and specify an option for the port Encap Type parameter.

The range for the Inner Encapsulation Value and the Outer Encapsulation Value parameters depend on the option you choose for the port Encap Type parameter.

- 15 Click on the Next button. The Create L2 Interface - Define General Properties form opens.

Configure the parameters.

- i Configure the interface Description parameter. The description can be up to 80 characters.
- ii Configure the interface Administrative State parameter. The options are Up or Down.

- 16 Click on the Next button. The Create L2 Interface - Select QoS Policies form opens, as shown in Figure 24-16.

Figure 24-16 Create L2 Interface - Select QoS Policies

- i Click on the Ingress: Select button to list and choose an access ingress policy.
 - ii Click on the Egress: Select button to list and choose an access egress policy.
- 17** Click on the Next button. The Create L2 Interface - Aggregation form opens.

Configure the Aggregation parameter. The parameter specifies whether an aggregation scheduler policy will be applied to the interface. The options are On or Off.

When you choose On, go to step 18 of this procedure.

When you choose Off, go to step 19 of this procedure.

- 18** Click on the Next button. The Create L2 Interface - Select Aggregation Scheduler Policy form opens.

Click on the Select button to list and choose an aggregation scheduler policy.

Go to step 20 of this procedure.

- 19** Click on the Next button. The Create L2 Interface - Select Ingress and Egress Scheduler Policies form opens.
- i Click on the Ingress: Select button to list and choose an ingress scheduler policy.
 - ii Click on the Egress: Select button to list and choose an egress scheduler policy.

- 20 Click on the Next button. The Create L2 Interface - Select ACL Filters form opens.
 - i Click on the Ingress: Select button to list and choose an ingress ACL filter.
 - ii Click on the Egress: Select button to list and choose an egress ACL filter.
- 21 Click on the Next button. The Create L2 Interface - Select Accounting Policy form opens.

Configure the parameters.

 - i Click on the Select button to list and choose an accounting policy.
 - ii Select the Accounting Enabled check box to enable the collection of accounting statistics for the interface.
- 22 Click on the Next button. The Create L2 Interface - Configure Spanning Tree Protocol form opens, as shown in Figure 24-17.

Figure 24-17 Create L2 Interface - Configure Spanning Tree Protocol form

Steps

1. Select Port
2. Define General Properties
3. Select QoS Policies
4. Aggregation
5. Select Ingress and Egress Scheduler Policies
6. Select ACL Filters
7. Select Accounting Policy
8. Configure Spanning Tree Protocol

Configure Spanning Tree Protocol

Properties

Path Cost: Port Number:

Priority: Rapid Start:

States

Administrative State:

< Back Next > Finish Cancel

Configure the parameters.

- i** Configure the Path Cost parameter. The parameter specifies the cost of the path to the root device as seen from this device. The range is 1 to 200 000 000.
- ii** Configure the Port Number parameter. The range is 0 to 4094.
- iii** Configure the Priority parameter. The parameter specifies the value of the port priority field which is contained in the most significant 4 bits of the 16-bit Port ID. The range is 0 to 255.
- iv** Configure the Rapid Start parameter. The parameter specifies whether rapid start is enabled on this interface, in the forwarding state. The options are Disabled or Enabled.
- v** Configure the Administrative State parameter. The options are Up or Down.

If you are configuring an interface on a 7450 ESS, go to step 23. Otherwise, go to step 24.

- 23** Click on the Next button. The Create L2 Interface - Configure FIB form opens. Configure the parameters.

- i** Configure the Aging Enabled parameter. The options are true or false.
- ii** Configure the Learning Enabled parameter. The options are true or false.
- iii** Configure the Maximum Entries parameter.

- 24** Click on the Finish button. The form you are configuring closes and the Create Service Site - Configure L2 Interfaces form re-opens. The interface and interface parameters are listed.

You can add, edit, or remove interfaces.

You can configure forwarding control parameters on the newly created L2 interface.

- i** Select an L2 interface from the list.
- ii** Click on the Edit button.

The L2 Interface properties form with the General tab appears.

- iii** Click on the Forwarding Control tab button. A series of additional tabs appears, as shown in Figure 24-18. The tabs and parameters that appear depend on the type of managed device, for example a 7450 ESS or 7750 SR.

Figure 24-18 L2 Interface properties form

The screenshot shows a configuration window for an L2 interface. The 'STP' tab is selected, and the 'Properties' section is visible. The 'Path Cost' is set to 10, 'Port Number' to 0, 'Priority' to 128, 'Rapid Start' to Disabled, 'Edge Capability Detection' to Enabled, and 'Link Type' to Point To Point. The 'Administrative State' is set to up. The window has standard navigation buttons at the bottom: Reset, OK, Cancel, and Apply.

- iv Click on the appropriate tab button to configure the parameters.
 - STP tab to configure spanning tree protocol settings for the L2 interface. The parameters include:
 - Path Cost. The range is 1 to 200 000 000.
 - Port Number. The range is 0 to 4094.
 - Priority. The range is 0 to 255.
 - Rapid Start. The options are Disabled or Enabled.
 - Edge Capability Detection. The parameter specifies whether the edge port characteristics of the access interface will be automatically detected. The options are Disabled or Enabled.
 - Link Type. The options are Point-to-Point or Shared.
 - FIB Entries tab to configure and manage FIB entries, as described in Procedure 24-5
 - v Click on the OK button. The L2 Interface form closes and the Create Service Site - Configure L2 Interfaces form re-opens.
- 25** Click on the Next button. The Create Service Site - Configure Spanning Tree Protocol form opens, as shown in Figure 24-19.

Figure 24-19 Create Service Site - Configure Spanning Tree Protocol form

Alcatel STP can be used within an VPLS to inter-operate with customer STP implementations as a mechanism for loop detection and prevention. The bridge-level parameters allow the balancing of TSTP between resiliency any speed of convergence extremes. Note that modifying the bridge-level parameters must be done in the constraints of the following two formulas:

- $2 \times (\text{Bridge_Forward_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge_Max_Age}$.
- $\text{Bridge_Max_Age} \geq 2 \times (\text{Bridge_Hello_Time} + 1.0 \text{ seconds})$

Configure the bridge-level parameters for the VPLS. Additional parameters may appear depending on the type of device that you are configuring.

- i Configure the Bridge Forward Delay (seconds) parameter. The range is 4 to 30 seconds
- ii Configure the Bridge Hello Time (seconds) parameter. The range is 1 to 10 seconds.
- iii Configure the Bridge Max Age (seconds) parameter. The range is 6 to 40 seconds.
- iv Configure the Priority parameter. The range is 0 to 65 535.
- v Configure the Administrative State parameter. The options are Up or Down.

- 26 Click on the Next button. The Create Service Site - Configure FIB form opens, as shown in Figure 24-20.

Figure 24-20 Create Service Site - Configure FIB form

Configure the parameters.

- i Configure the High Watermark (%) parameter. The high and low watermark parameters specify when alarms are raised based on whether the FIB is reaching the maximum number of MAC addresses it can contain. The range is 0 to 100.
 - ii Configure the Low Watermark (%) parameter. The range is 0 to 100.
 - iii Configure the Local Age Time (seconds) parameter. The parameter specifies the number of seconds to age out FIB entries on access interfaces. The range is 60 to 86 400 seconds.
 - iv Configure the Remote Age Time (seconds) parameter. The parameter specifies the number of seconds to age out FIB entries on circuits. The range is 60 to 86 400 seconds.
 - v Configure the Size (entries) parameter. The parameter specifies the number of learned and static entries in the FIB. The range is 1 to 131 071.
 - vi Select the Aging Enabled check box to allow enable for the FIB.
 - vii Select the Learning Enabled check box to enable learning for the FIB.
 - viii Select the Discard Unknown Destinations check box to specify whether traffic from unknown destination MAC addresses is handled or discarded.
- 27** Click on the Finish button. The Create Service Site - Configure FIB form closes and the Create Service - Configure Sites form re-opens. The site and the site parameters are listed. The tabs and parameters that appear depend on the type of managed device, for example a 7450 ESS or 7750 SR.

You can add, edit, or remove sites.

You can configure forwarding control parameters on the newly created site.

- i** Select a site from the list.
 - ii** Click on the appropriate tab button to configure the parameters.
 - Site STP tab to configure spanning tree protocol settings for the site. The parameters include:
 - RSTP Type to specify the type of spanning tree protocol for the site. This parameter applies to 7450 ESS sites. The options are RSTP (default), CompDot1w and Dot1w.
 - Maximum BPDUs (PDUs/Hello Interval) to specify the maximum number of BPDUs. This parameter applies to 7450 ESS sites. The range is 1 to 10.
 - Bridge Forward Delay (seconds). The range is 4 to 30 seconds
 - Bridge Hello Time (seconds). The range is 1 to 10 seconds.
 - Bridge Max Age (seconds). The range is 6 to 40 seconds.
 - Priority. The range is 0 to 65 535.
 - L2 Interface STP tab to configure spanning tree protocol settings for the interfaces.
 - Circuit STP tab to configure spanning tree protocol settings for the access spoke circuits.
 - FIB tab to configure FIB parameters for the site.
 - FIB Entries tab to configure and manage FIB entries, as described in Procedure 24-5.
 - Statistic tab which displays STP and FIB statistics.
 - iii** Click on the OK button to save the changes.
 - iv** Verify the action, if required.
- 28** Click on the Next button. The Create Service - L2 Interfaces Summary form opens as shown in Figure 24-21.

Figure 24-21 Create Service - L2 Interfaces Summary form

Interface and interface parameters are listed. You can add, edit, or remove interfaces.

- 29 Click on the Next button.
 - a If you chose Manual: User Defined Connectivity in step 7, the Create Service - Configure Circuits form opens. Go to step 30.
 - b If you chose All Access Sites Fully Meshed (No Hierarchy) in step 7, the Circuits Summary form opens. Circuits are automatically created and associated with the service. Go to step 38.
- 30 In the Create Service - Configure Circuits form, click on the Add button. The Create Circuit - Select Source Node form appears as shown in Figure 24-22. Choose a source node.

Figure 24-22 Create Circuit - Select Source Node form

Steps

1. Select Source Node
2. Select Destination Node
3. Select Tunnel
4. Define General Properties
5. Define VC Properties
6. Select ACL Filters

Select Source Node

Site ID ▾	Site Name	Description	Admin
38.120.182.21	138.120.182.21		Up
38.120.182.23	138.120.182.23		Up

Source Node ID: Source Node Name:

< Back Next > Finish Cancel

- 31 Click on the Next button. The Create Circuit - Select Destination Node form opens.
 - a If the destination node is a managed site, choose a site from the list.
 - b If the destination node is an unmanaged site, specify the system ID for the Destination Node ID parameter.
- 32 Click on the Next button. The Create Circuit - Select Tunnel form opens.

Click on the Select button to list and choose a tunnel, if required. A tunnel can be dynamically created by the 5620 SAM.
- 33 Click on the Next button. The Create Circuit - Define General Properties form opens.

Configure the circuit Administrative State parameter. The options are Up or Down.
- 34 Click on the Next button. The Create Circuit - Define VC Properties form opens.

Configure the parameters.

- To have the 5620 SAM automatically assign a VC ID, select the Auto-Assign ID check box.
 - To manually assign a VC ID, deselect the Auto-Assign ID check box.
 - Configure the VC ID parameter. The range is 1 to 2 147 483 647
 - Configure the VC Type parameter. The parameter specifies the default VC type signaled for the circuit to service tunnel binding to the far end of a mesh service tunnel. The actual signaling of the VC type depends on the signaling parameter defined for the service tunnel. The options are Undefined, Ethernet, VPLS, or VLAN.
 - Configure the VLAN VC Tag parameter. The parameter specifies an explicit dot1q value for encapsulation to the far end of the service tunnel. The range is 0 to 4094.
- 35** Click on the Next button. The Create Circuit - Select ACL Filters form opens.
 - i** Click on the Ingress: Select button to list and choose an ingress ACL filter.
 - ii** Click on the Egress: Select button to list and choose an egress ACL filter.
- 36** Click on the Finish button. The Create Circuit - Select ACL Filters form closes and the Create Service - Configure Circuits form re-opens.

You can list the circuits and view circuit parameters in the circuit list that appears at the bottom of the form. Choose the Unidirectional or Bidirectional parameter and selecting routers from the To and/or From lists. The circuits that appear in the circuits list are filtered according to the criteria you specify.

You can add, edit, or remove circuits.

- 37** Click on the Next button. The Create Service - Circuits Summary form opens. Circuits and circuit parameters are listed in the form.

If required, you can add, edit, or remove circuits.

- i** Select a circuit from the list.
- ii** Click on the Edit button.

The Circuit (Create) properties form with the General tab appears.

- iii** Configure the Type parameter to specify the type of circuit. The options are Spoke or Mesh.

When you choose Spoke, the Forwarding Control tab button appears.

- iv** Click on the Forwarding Control tab button.
- v** Click on the STP tab button to configure spanning tree protocol settings for the L2 interface. The parameters include:
 - Path Cost. The range is 1 to 200 000 000.
 - Port Number. The range is 0 to 4094.
 - Priority. The range is 0 to 255.
 - Rapid Start. The options are Disabled or Enabled.
 - Edge Capability Detection. The parameter specifies whether the edge port characteristics of the access interface will be automatically detected. The options are Disabled or Enabled.
 - Link Type. The options are Point-to-Point or Shared.
- vi** Click on the OK button to save the changes.
- vii** Close the form.

The modified parameters for the circuit appear in the list.

- 38** Click on the Finish button. The Create Service - Circuits Summary form closes and the Subscriber Manager form re-opens. The service and service parameters are listed in the form.

You can add, edit or remove services.

- 39** Click on the Apply button to save the service.
-

Procedure 24-2 To modify a VPLS

- 1** Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu.
- 2** Configure the subscriber list filter parameters and click on the Search button. A list of available subscribers appears at the bottom of the Subscriber Manager form.
- 3** Choose a subscriber from the list.
- 4** Click on the Edit button. The Subscriber form with the General tab opens.
- 5** Click on the Services tab. A list of services appears.
- 6** Choose a service.
- 7** Click on the Edit button. A Service edit form with the General tab opens.

- 8 Modify the parameters for the service as required.



Caution — Modifying parameters can be service-affecting.

The parameter information that appears for the service includes:

- General tab that displays the general properties of the service
 - Transport tab that displays the transport information for the service
 - Forwarding Control tab that displays FIB and spanning tree protocol information
 - Sites tab that lists the sites included in the service
 - L2 Interface tab that lists interfaces used by the service
 - Circuits tab (circuits are VC IDs bound to service tunnels) that lists the circuits that are used by the customer. A Mesh tab and a Spoke tab are available from the Circuits tab form. You can add mesh circuits from the Mesh tab. You can create access spokes for HVLPS from the Spoke tab, as described in Procedure 24-4.
 - Maintenance tab that lists OAM diagnostics that can be performed to diagnose the service
 - Faults tab that displays faults associated with the service
- 9 Click on the OK button to close the Service edit form. The Subscriber form re-opens.
 - 10 Click on the Apply button to save the modified service.
-

Procedure 24-3 To delete a VPLS

- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu.
 - 2 Configure the subscriber list filter parameters and click on the Search button. A list of available subscribers appears at the bottom of the Subscriber Manager form.
 - 3 Choose a subscriber from the list.
 - 4 Click on the Edit button. The Subscriber form with the General tab opens.
 - 5 Click on the Services tab. A list of services appears.
 - 6 Choose a service.
 - 7 Click on the Remove button. The service is removed from the list.
 - 8 Click on the Apply button to delete the service.
-

Procedure 24-4 To configure HVPLS using access spoke circuits

Perform this procedure to interconnect a VLL, VPLS, or service site to a VPLS using access spoke circuits. The VPLS to VPLS, VPLS to VLL, or VPLS to service site interconnection is referred to as an HVPLS.

- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu.
- 2 Configure the subscriber list filter parameters and click on the Search button. A list of available subscribers appears at the bottom of the Subscriber Manager form.
- 3 Choose a subscriber from the list whose service needs an access spoke circuit added to create an HVPLS.
- 4 Click on the Edit button. The Subscriber form with the General tab opens.
- 5 Click on the Circuits tab.
- 6 Click on the Spoke tab.
- 7 Click on the Add button.

The Create Circuit - Select Source form opens as shown in Figure 24-23.

Figure 24-23 Create Circuit - Select Source form

The screenshot shows a web-based form titled "Create Circuit - 0.0.0.0, Subscriber - 5". On the left, a "Steps" sidebar lists nine steps, with "1. Select Source" highlighted in blue. The main content area is titled "Select Source" and contains the text "Do you want to create a new service, or start with an existing service?". Below this text are two radio buttons: "Create New Service" (which is unselected) and "Use Existing Service" (which is selected). At the bottom of the form, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Choose whether you want to create a new service, or use an existing service, to connect to an existing VPLS using an access spoke circuit.

If you choose to create a new service, go to step 8 of this procedure.

If you choose to use an existing service, go to step 10 of this procedure.

- 8** Click on the Next button. The Create Circuit - Select Service Type form opens.

Configure the parameters.

- i** Choose whether you want to create a new VLL or VPLS service.
- ii** Configure the Transport Preference parameter. The options are Any, GRE, or MPLS:RSVP-LSP.



Note — To use MPLS as the transport type, you must bind LSPs to service tunnels during service tunnel configuration. See Procedure 19-1 for more information.

- iii** Configure the Use Bw Reserved Paths parameter. The options are No Preference, never, or always.

- 9** Click on the Next button. The Create Circuit - Create L2 Interfaces form opens. You must create at least one interface for the VLL or VPLS you are creating. The interface is on the router which is not shared by the two VPLSs, or by the VPLS and the VLL service.

If you are creating an interface for a VLL, create the interface as described in Procedure 23-1 in section 23.6.

If you are creating an interface for a VPLS, create the interface as described in Procedure 24-1 in this section.

After you have created the interface, go to step 11 of this procedure.

- 10** Click on the Next button. The Create Circuit - Select Service form opens. Choose the service that will contain the circuit that you are creating.

- 11** Click on the Next button. The Create Circuit - Select Source Node form opens. Choose a source node for the circuit you are creating.

- 12** Click on the Next button. The Create Circuit - Select Destination window opens.

Choose whether you want the destination to be a VPLS service or a device (site ID).

If you choose VPLS service, go to step 13 of this procedure.

If you choose a device (site ID), go to step 14 of this procedure.

- 13** Click on the Next button. The Create Circuit - Select Destination Service form opens. Choose a destination service.

- 14** Click on the Next button. The Create Circuit - Select Destination Node form opens.

- a** If the destination node is a managed site, choose a site from the list.
- b** If the destination node is an unmanaged site, specify the system ID for the Destination Node ID parameter.

- 15** Click on the Next button. The Create Circuit - Select Tunnel form opens. Configure the parameters.

- 19 Click on the Next button. The Create Circuit - Configure STP form opens. Configure the parameters for the source node.
 - i Configure the Path Cost parameter. The range is 1 to 200 000 000.
 - ii Configure the Port Number parameter. The range is 0 to 4094.
 - iii Configure the Priority parameter. The range is 0 to 255.
 - iv Configure the Rapid Start parameter. The parameter specifies whether rapid start is enabled on this interface, in the forwarding state. The options are Disabled or Enabled.
 - v Configure the Administrative State parameter. The options are Up or Down.

If the source node for the circuit is a 7450 ESS, go to step 20 of this procedure.

If the source node for the circuit is a 7750 SR, go to step 21 of this procedure.
 - 20 Click on the Next button. The Create Circuit - Configure FIB form opens.

Configure the parameters for the source node.

 - i Configure the Aging Enabled parameter. The options are true or false.
 - ii Configure the Learning Enabled parameter. The options are true or false.
 - iii Configure the Maximum Entries parameter.
 - 21 Click on the Finish button. The Create Circuit form closes and the Subscriber form with the Circuits tab re-opens after you confirm the action.
 - 22 Click on the Apply button to save your configuration.
-

Procedure 24-5 To add or modify FIB entries

You can create and manage FIBs:

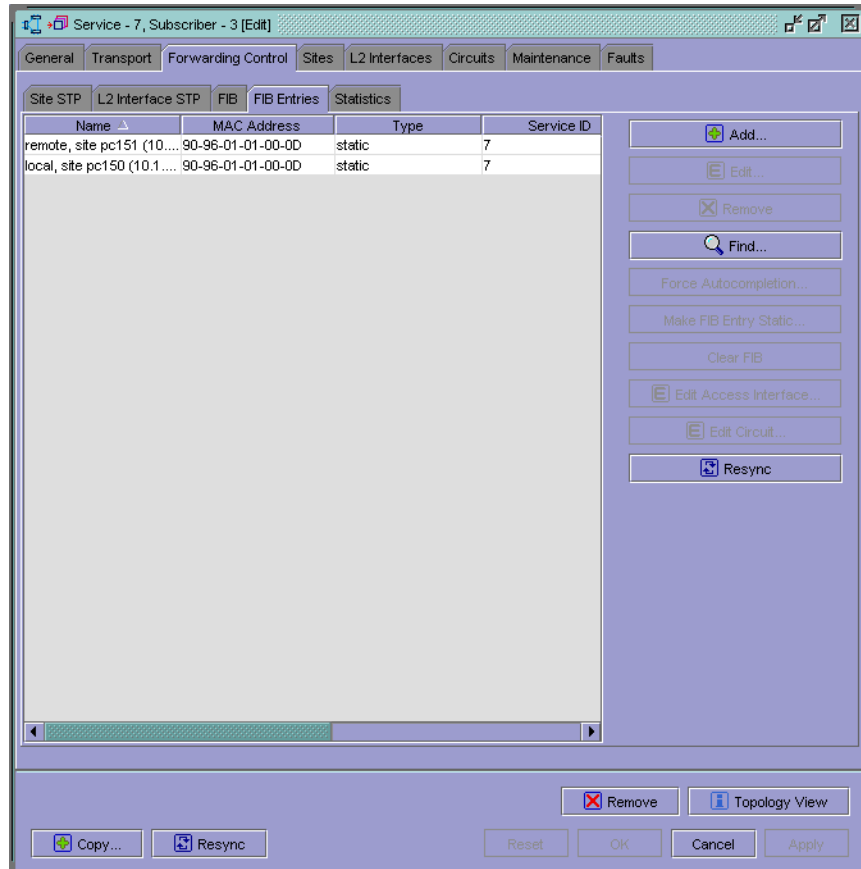
- from the global FIB entries form
- for each subscriber
- per service site
- for each access interface
- for each circuit

Use the following procedure to add or modify FIB entries using the subscriber FIB entry form.

- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu.
- 2 Configure the subscriber list filter parameters and click on the Search button. A list of available subscribers appears at the bottom of the Subscriber Manager form.
- 3 Choose a subscriber from the list.

- 4 Click on the Edit button. The Subscriber form with the General tab opens.
- 5 Click on the Forwarding Control tab.
- 6 Click on the FIB Entries tab.
- 7 Click on the Find button. A list of FIB entries appears in the FIB Entries tab, as shown in Figure 24-24.

Figure 24-24 FIB Entries tab



- 8 Add or modify FIB entries as required.
 - a To add FIB entries:
 - i Click on the Add button in the FIB Entries tab. The FIB Entry form appears as shown in Figure 24-25.

Figure 24-25 FIB Entry form

Site ID	Site Name	Service ID	Service Name	Ser
10.1.1.150	pc150	7	VPLS service-7: Site ...	VPLS
10.1.1.151	pc151	7	VPLS service-7: Site ...	VPLS

- ii Configure the MAC Address and Auto-Complete parameters as required.
 - iii Choose an interface or circuit from the list in the L2 Interfaces or the Services Circuits tab.
 - iv Click on the Apply button to save the entry.
- b** To modify FIB entries:
- i Choose a FIB entry from the FIB Entries tab.
 - ii Modify the FIB entry as required.

You can view additional FIB entry information, including faults, and modify some parameters, by choosing the FIB entry and clicking on the Edit button.

Procedure 24-6 To view the service topology

- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu.
- 2 Configure the subscriber list filter parameters and click on the Search button. A list of available subscribers appears at the bottom of the Subscriber Manager form.
- 3 Choose a subscriber from the list.
- 4 Click on the Edit button. The Subscriber form with the General tab opens.
- 5 Click on the Services tab. A list of services appears.
- 6 Choose a service.

- 7 Click on the Edit button. A Service edit form with the General tab opens.
 - 8 Click on the Topology view button. The service topology map opens.
-

25 — IES management

- 25.1 IES management overview 25-2**
- 25.2 Sample IES configuration 25-3**
- 25.3 Workflow to create an IES 25-5**
- 25.4 IES management menus 25-5**
- 25.5 IES management procedures list 25-5**
- 25.6 IES management procedures 25-6**

25.1 IES management overview

An IES is a routed connectivity service where the subscriber communicates with an IP router interface, which is a Layer 3 interface, to send and receive Internet traffic.

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 subscriber be unique among other provider addressing schemes and potentially the entire Internet.

You specify, configure, and modify access interfaces for a service when you configure or modify a service.

Packets arriving at the edge 7750 SR are associated with an IES based on the access interface on which they arrive. An access interface is uniquely identified by the:

- port
- service ID
- IP address

The 5620 SAM supports IES configuration through a sequence of configuration forms and steps. To create a service, choose a subscriber from the Service Management→Manage Subscribers/Services form and configure a service for the chosen subscriber. Figure 25-1 shows the Create Service form with the Define Service Type parameters displayed and IES chosen as the service type.

Figure 25-1 IES main service creation - Define Service Type form

The screenshot displays the 'Define Service Type' configuration form. On the left, a 'Steps' sidebar lists three steps: '1. Define Service Type' (highlighted), '2. Configure Sites', and '3. L3 Interfaces Summary'. The main form area contains the following fields and controls:

- Service ID:** A text input field containing the value '0'. To its right is a checked checkbox labeled 'Auto-Assign ID'.
- Service Name:** A text input field containing the value 'IES service'.
- Description:** A text input field containing the value 'What the service provides'.
- Type:** A dropdown menu with 'IES' selected.

At the bottom of the form, there are four navigation buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

Common to all 7750 SR 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 7750 SR 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.
- Scheduler policies to define hierarchical rate limiting and scheduling to govern the scheduling of queues. Scheduler policies are configured using the Scheduler Policy Manager.
- Filter policies to control network traffic into or out of an interface based on IP or MAC filtering 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.

See chapter 20 for more information about policies.

See chapter 29 for more information about performing OAM diagnostics on a per-service basis.

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 subscriber-owned IP interfaces. More than one IES can be created for one subscriber. More than one IP interface can be created in one IES. All IP interfaces created in an IES belong to the same subscriber.

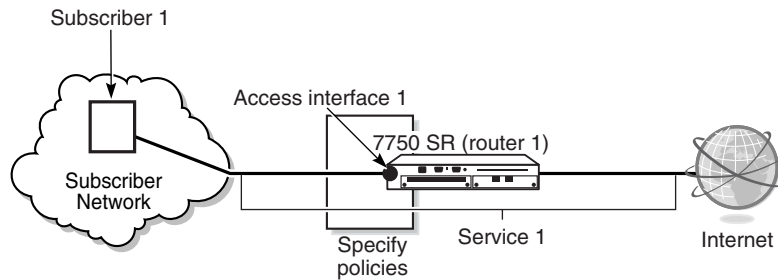
The IES IP interfaces are restricted to the routing protocols that can be defined on the interface based on the fact that the customer has a different routing domain for this service. The IP interfaces support the following routing protocols:

- RIP
- OSPF
- BGP
- IS-IS

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.

25.2 Sample IES configuration

Figure 25-2 shows a sample IES configuration.

Figure 25-2 Sample IES configuration

17233

The following table lists the high-level tasks necessary to configure this sample IES.

Table 25-1 Sample IES configuration

Task	Description
1. Configure policies as required	<p>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.</p> <ul style="list-style-type: none"> • QoS access ingress and egress interface policies. Choose Policies→Access Ingress Policy or Policies→Access Egress Policy to open these forms. • Scheduler policy. Choose Policies→Scheduler Policy Manager to open the scheduler policy form. • ACL IP filter policies. Choose Policies→Acl IP Filter Manager to open the IP filter form. • Accounting policy. Choose Policies→Accounting Policy to open the accounting policy form.
2. Create and configure Subscriber 1	<p>Choose Service Management→Manage Subscribers/Services to open the subscriber manager form and create a subscriber.</p>
3. Create and configure Service 1	<p>Click on the Services tab on the subscriber manager form and click on the Add button to create a new service. A series of steps, substeps, and forms guide you through the service creation process. You configure the following key elements when you configure Service 1.</p> <ul style="list-style-type: none"> • Choose Subscriber 1 as the subscriber for the IES. • Define the service type as IES. • Choose Router 1 as the site for the IES. • Configure and choose L3 access interface 1 as the access interface for the IES. You do the following when you configure access interfaces: <ul style="list-style-type: none"> • Specify the router (site). This is router 1 in the example. • Specify the port for the access interfaces. In the example, this would be access interface 1. Ports must be configured as access ports. Ports can be configured as dot1q. The specification of the customer ID, the port ID, and the Encap (VLAN ID) for the dot1q port defines the SAP. • Specify the IP address for the IES, one primary IP address and, optionally, multiple secondary IP addresses • Specify service-specific QoS ingress and egress policies • Specify service-specific IP ACL filters for the ingress and egress to control traffic, on the basis of IP addresses or classification of packets, to the customer • Specify if the access interfaces will participate in aggregation rate limiting across a card or port. If aggregation is not required, specify the participation of access interfaces in ingress and egress scheduler policies. If aggregation is required, specify the participation of access interfaces in an aggregation scheduler policy. • Specify ICMP parameters to control messaging and error reports, and to provide information relevant to IP packet processing

25.3 Workflow to create an IES

- 1 Set up group and user access privileges.
- 2 Configure the network:
 - i Build the IP core network. You do not need an IP/MPLS network for IESs.
 - ii Configure routing protocols.
 - iii Have access ports available on the router.
- 3 Configure new or choose existing QoS, filter, and accounting policies.
- 4 Provision the service:
 - i Set up subscribers or associate existing subscribers with new services.
 - ii Configure customer-specific QoS, filter, scheduling, and accounting policies, or use pre-defined policies.
 - iii Create the IES. The sample parameters are listed in Table 25-1.
 - Define the service type as IES
 - Choose a router (site)
 - Configure the IP interface
 - Associate an access port with the IP interface
 - Specify policies for the service, such as QoS
- 5 Turn up the service.

25.4 IES management menus

Table 25-2 lists and describes the 5620 SAM IES menus.

Table 25-2 IES service management menus

Menu item	Description
Service Management→Manage Subscribers/Services	Create and manage subscribers and the services that they are using.
Service Management→Create Service	Create an IES for subscribers to communicate with an IP router interface to send and receive Internet traffic.
Service Management→Browse Services	Perform a filtered search on services to find the configured IES.

25.5 IES management procedures list

Table 25-3 lists the procedures necessary to perform IES service management tasks.

Table 25-3 IES service procedures list

Procedure	Purpose
To create an IES	Create an EIS for subscribers to communicate with an IP router interface to send and receive Internet traffic.
To modify an IES	Modify an IES
To delete an IES	Delete an IES
To view the service topology	View a graphical representation of an IES that shows the site and interfaces.

25.6 IES management procedures

Use the following procedures to perform IES creation and management tasks. See the *7750 SR OS Services Guide* for more information about IES configuration and parameters.

Procedure 25-1 To create an IES

This procedure describes how to create an IES using the Subscriber Manager form as the starting point. This allows you to browse a list of subscribers, and choose a subscriber for the service before you start creating the service.

You can also create an IES service using the Create Service form as the starting point. This allows you to choose a subscriber for the service during service configuration. Choose Service Management→Create Service from the 5620 SAM main menu.

- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu. The Subscriber Manager form opens, as shown in Figure 25-3.

Figure 25-3 Subscriber Manager form

Subscriber Manager

Search Filter Type: Simple

Unused Properties:

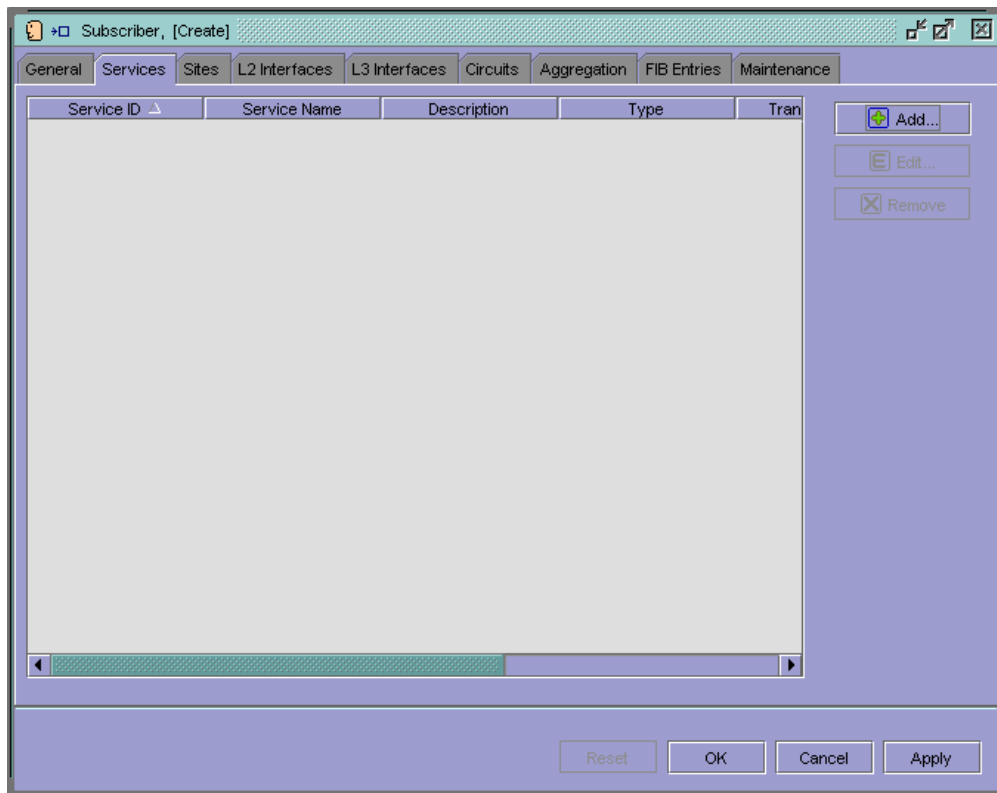
- Address
- Contact
- Description
- Email
- ID
- Name
- Phone Number

Filtered Properties:

Create Subscriber... Search Cancel

- 2 Configure the subscriber list filter parameters and click on the Search button. A list of available subscribers appears at the bottom of the Subscriber Manager form.
- 3 Choose a subscriber from the list to use the IES you are creating.
- 4 Click on the Edit button. The Subscriber form with the General tab opens.
- 5 Click on the Services tab. Figure 25-4 shows the Subscriber form with the Services tab button selected.

Figure 25-4 Subscriber form — Services



- 6 Click on the Add button. The Create Service - Define Service Type form opens, with VPLS chosen as the default service type, as shown in Figure 25-5.

Figure 25-5 Create Service - Define Service Type form

Configure the parameters.

- i Specify how you want service IDs assigned. The ID uniquely identifies the service in the service domain.
 - To have the 5620 SAM automatically assign a service ID, select the Auto-Assign ID check box.
 - To manually assign a service ID, deselect the Auto-Assign ID check box. Configure the Service ID parameter. The range is 1 to 2 147 483 647
- ii Configure the Service Name parameter. The name can be up to 32 characters.
- iii Configure the service Description parameter. The description can be up to 80 characters.
- iv Choose IES for the Type parameter. The series of steps to create the IES service appears, as shown in Figure 25-6.

Figure 25-6 Create Service - Define Service Type form

The screenshot shows a web-based form titled "Create Service - Subscriber - 1". On the left, a "Steps" sidebar lists: 1. Define Service Type (highlighted), 2. Configure Sites, and 3. L3 Interfaces Summary. The main area is titled "Define Service Type" and contains the following fields:

- Service ID: Auto-Assign ID
- Service Name:
- Description:
- Type:

At the bottom right, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

- 7 Click on the Next button. The Create Service - Configure Sites form opens.
- 8 Click on the Add button. The Create Service Site - Number of Sites form opens, as shown in Figure 25-7.

Figure 25-7 Create Service Site - Number of Sites form

Choose Single from the drop-down menu to add and configure a single site. After you configure the site, you can add and configure additional sites.



Note — You can add and configure multiple sites at the same time. Choose Multiple from the drop-down menu and follow the series of steps that appears.

- 9 Click on the Next button. The Create Service Site - Select Site form opens.
Click on the Select button to list and choose a site.
- 10 Click on the Next button. The Create Service Site - Define General Properties form opens.
Configure the parameters.
 - i Configure the site Description parameter. The description can be up to 80 characters.
 - ii Configure the site Administrative State parameter. The options are Up or Down.
- 11 Click on the Next button. The Create Service Site - Configure L3 Interfaces form opens, as shown in Figure 25-8.

Figure 25-8 Create Service Site - Configure L3 Interfaces

- 12 Click on the Add button. The Create L3 Interface - Define General Properties form opens, as shown in Figure 25-9.

Figure 25-9 Create L3 Interface - Define General Properties form

Configure the parameters.

- i** Specify how you want interface IDs assigned. The ID uniquely identifies the interface in the service domain.
 - To have the 5620 SAM automatically assign an interface ID, select the Auto-Assign ID check box.
 - To manually assign an interface ID, deselect the Auto-Assign ID check box. Configure the Interface ID parameter. The range is 2 to 5119.
 - ii** Configure the interface Name parameter. The name can be up to 32 characters.
 - iii** Configure the interface Description parameter. The description can be up to 80 characters.
 - iv** Configure the interface Administrative State parameter. The options are Up or Down.
 - v** Specify a MAC address for the interface for the MAC Address parameter.
 - vi** Select the Allow Direct Broadcasts check box to enable the forwarding of direct broadcasts from the interface.
 - vii** Select the Loopback Enabled check box to enable loopbacks on the interface.
 - viii** Configure the Cflowd Type parameter. The options are None, ACL, or Interface.
- 13** Click on the Next button. The Create L3 Interface - Configure IP Address form opens.
 - 14** Click on the Add button. The IP Address form opens, as shown in Figure 25-10.

Figure 25-10 IP Address form

Configure the parameters.

- i Specify an interface IP address for the IP Address parameter.
- ii Specify a mask for the Subnet Mask parameter.
- iii Specify a format for the Broadcast Address Format parameter. The options are All Ones or Host Ones.
- iv Select the Primary check box if you want the IP address to be the primary IP address for the interface.

After you assign a primary IP address to the interface, you can assign multiple secondary IP addresses to the interface. Repeat this step and deselect the Primary check box to assign additional IP addresses to the interface.

- 15 Click on the OK button. The IP Address form closes and the Create L3 Interface - Configure IP Address form re-opens. The IP address and other parameters are displayed in the form.
- 16 Click on the Next button. The Create L3 Interface - Select Port form opens, as shown in Figure 25-11.

Figure 25-11 Create L3 Interface - Select Port form

Configure the parameters.

- i Click on the Select button to list and choose a port or channel.

You can only choose ports or channels in access mode. Use the 5620 SAM navigation tree to choose a port or channel and set the Mode parameter to Access.

After you choose a port or channel, additional steps to configure the interface appear, as shown in Figure 25-12.

Figure 25-12 Create L3 Interface - Select Port form

The screenshot shows a web-based configuration interface for creating a Layer 3 interface. The window title is "Create L3 Interface - 10.1.1.18, Subscriber - 2". On the left, a "Steps" sidebar lists 10 steps, with "3. Select Port" highlighted. The main area is titled "Select Port" and contains the following fields and buttons:

- Port: Channel 8/2/1_ds3e3-1.1 (with "Select..." and "View..." buttons)
- Port ID: 675315778
- Encap Type: BCP Null
- Outer Encapsulation Value: 0
- Inner Encapsulation Value: 0
- A "Remove" button with a red X icon.

At the bottom of the form, there are four navigation buttons: "< Back", "Next >", "Finish", and "Cancel".

- ii Configure the Inner Encapsulation Value and the Outer Encapsulation Value parameters.

One or both parameters are configurable when the port encapsulation type is Dot1q, Q in Q, BCP Dot 1q, or FR. Use the 5620 SAM navigation tree to choose a port or channel and specify an option for the port Encap Type parameter.

The range for the Inner Encapsulation Value and the Outer Encapsulation Value parameters depend on the option you choose for the port Encap Type parameter.

- 17 Click on the Next button. The Create L3 Interface - Select QoS Policies form opens, as shown in Figure 25-13.

Figure 25-13 Create L3 Interface - Select QoS Policies form

- i Click on the Ingress: Select button to list and choose an access ingress policy.
 - ii Click on the Egress: Select button to list and choose an access egress policy.
- 18** Click on the Next button. Click on the Next button. The Create L3 Interface - Aggregation form opens.

Configure the Aggregation parameter. The parameter specifies whether an aggregation scheduler policy will be applied to the interface. The options are On or Off.

When you choose On, go to step 19 of this procedure.

When you choose Off, go to step 20 of this procedure.

- 19** Click on the Next button. The Create L3 Interface - Select Aggregation Scheduler Policy form opens.

Click on the Select button to list and choose an aggregation scheduler policy.

Go to step 21 of this procedure.

- 20** Click on the Next button. The Create L3 Interface - Select Ingress and Egress Scheduler Policies form opens

- i Click on the Ingress: Select button to list and choose an ingress scheduler policy.
- ii Click on the Egress: Select button to list and choose an egress scheduler policy.

- 21 Click on the Next button. The Create L3 Interface - Select ACL Filters form opens.
 - i Click on the Ingress: Select button to list and choose an ingress ACL filter.
 - ii Click on the Egress: Select button to list and choose an egress ACL filter.
- 22 Click on the Next button. The Create L3 Interface - Select Accounting Policy form opens.

Configure the parameters.

 - i Click on the Select button to list and choose an accounting policy.
 - ii Select the Accounting Enabled check box to enable the collection of accounting statistics for the interface.
- 23 Click on the Next button. The Create L3 Interface - Configure ICMP form opens, as shown in Figure 25-14.

Figure 25-14 Configure ICMP form

Steps

1. Define General Properties
2. Configure IP Address
3. Select Port
4. Select QoS Policies
5. Aggregation
6. Select Ingress and Egress Scheduler Policies
7. Select ACL Filters
8. Select Accounting Policy
9. Configure ICMP
10. Configure ARP

Configure ICMP

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):

< Back Next > Finish Cancel

Configure the parameters.

- i Select the Mask Reply check box to enable responses to the ICMP mask requests on the router interface.
 - ii Select the Redirects check box to enable configuration of rates for ICMP redirect messages on the router interface. Redirects are issued by the router when the router determines that a more optimal route is available.
 - iii Configure the Number of Redirects parameter. The range is 10 to 1000.
 - iv Configure the Redirects Time (seconds) parameter. The range is 1 to 60.
 - v Select the Unreachables check box to enable the configuration of the rate for ICMP host and network destination unreachable messages issued on the router interface.
 - vi Configure the Number of Unreachables parameter. The range is 10 to 1000.
 - vii Configure the Unreachables Time (seconds) parameter. The range is 1 to 60.
 - viii Select the TTL Expired check box to enable the rate of ICMP TTL expired messages issued by the router interface.
 - ix Configure the Number of TTL Expired parameter. The range is 10 to 1000.
 - x Configure the TTL Expired Time (seconds) parameter. The range is 1 to 60.
- 24** Click on the Next button. The Create L3 Interface - Configure ARP form opens, as shown in Figure 25-15.

Figure 25-15 Create L3 Interface - Configure ARP form

The screenshot shows the 'Create L3 Interface - Configure ARP' form. On the left, a 'Steps' sidebar lists 10 steps, with '10. Configure ARP' highlighted in blue. The main content area is titled 'Configure ARP' and features a 'Timeout' input field with the value '14400'. Below the timeout field is a table with four columns: 'Site ID', 'Site Name', 'Routing Instance ID', and 'Routing Instance Name'. The table is currently empty. To the right of the table are three buttons: 'Add...' (with a plus icon), 'Edit...' (with a pencil icon), and 'Remove' (with a minus icon). At the bottom of the form are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

Configure the ARP Timeout parameter. The parameter specifies, in seconds, how long an ARP entry is maintained without being refreshed. The range is 0 to 65 535.

- 25** To add static ARP entries, click on the Add button. The Static ARP form opens.

Configure the parameters.

- i** Specify an IP address for the IP Address parameter.
- ii** Specify a physical address, in the format *xx-xx-xx-xx-xx*, for the Physical Address parameter.

- 26** Click on the OK button. The Static ARP form closes and the Create L3 Interface - Configure ARP form re-opens. The IP address and other parameters are listed in the form.

- 27** Click on the Finish button. The Create L3 Interface - Configure ARP form closes and the Create Service Site - Configure L3 Interfaces form re-opens. The interface and interface parameters are listed in the form.

You can add, edit, or remove interfaces.

- 28** Click on the Finish button. The Create Service Site - Configure L3 Interfaces form closes and the Create Service - Configure Sites form re-opens. The site and the site parameters are listed.

You can add, edit, or remove sites.

- 29** Click on the Next button. The Create Service - L3 Interfaces Summary form opens, as shown in Figure 25-16.

Figure 25-16 Create Service - L3 Interfaces Summary form

Service ID	Service Name	Service Type	Site ID
0		IES	10.1.1.18

Interface and interface parameters are listed. You can add, edit, or remove interfaces.

- 30 Click on the Finish button. The Create Service - L3 Interfaces Summary form closes and the Subscriber Manager form re-opens. The service and service parameters are listed in the form.
 - 31 Click on the Apply button to save the service.
-

Procedure 25-2 To modify an IES

- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu.
- 2 Configure the subscriber list filter parameters and click on the Search button. A list of available subscribers appears at the bottom of the Subscriber Manager form.
- 3 Choose a subscriber from the list.
- 4 Click on the Edit button. The Subscriber form with the General tab opens.
- 5 Click on the Services tab. A list of services appears.
- 6 Choose a service.
- 7 Click on the Edit button. A Service edit form with the General tab opens.
- 8 Modify the parameters for the service as required.



Caution — Modifying parameters can be service-affecting.

The parameter information that appears for the service includes:

- General tab that displays the general properties of the service
 - Sites tab that lists the sites included in the service
 - L3 Interface tab that lists interfaces used by the service
 - Addresses tab
 - Faults tab that displays faults associated with the service
- 9 Click on the OK button to close the Service edit form. The Subscriber form re-opens.
 - 10 Click on the Apply button to save the modified service.
-

Procedure 25-3 To delete an IES

- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu.

- 2 Configure the subscriber list filter parameters and click on the Search button. A list of available subscribers appears at the bottom of the Subscriber Manager form.
 - 3 Choose a subscriber from the list.
 - 4 Click on the Edit button. The Subscriber form with the General tab opens.
 - 5 Click on the Services tab. A list of services appears.
 - 6 Choose a service.
 - 7 Click on the Remove button. The service is removed from the list.
 - 8 Click on the Apply button to delete the service.
-

Procedure 25-4 To view the service topology

- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu.
 - 2 Configure the subscriber list filter parameters and click on the Search button. A list of available subscribers appears at the bottom of the Subscriber Manager form.
 - 3 Choose a subscriber from the list.
 - 4 Click on the Edit button. The Subscriber form with the General tab opens.
 - 5 Click on the Services tab. A list of services appears.
 - 6 Choose a service.
 - 7 Click on the Edit button. A Service edit form with the General tab opens.
 - 8 Click on the Topology view button. The service topology map opens.
See chapter 27 for more information about service topology views.
-

26 — VPRN service management

- 26.1 VPRN service management overview 26-2**
- 26.2 Sample VPRN configuration 26-4**
- 26.3 Workflow to create a VPRN service 26-6**
- 26.4 VPRN service management menus 26-7**
- 26.5 VPRN service management procedures list 26-7**
- 26.6 VPRN service management procedures 26-8**

26.1 VPRN service management overview

The 5620 SAM supports the creation of VPRN services using the 7750 SR as a PE and provider core (P) router. VPRNs, which are also called IP VPNs or BGP/MPLS VPNs, are defined in RFC 2547bis. This standard details 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.

The 5620 SAM supports VPRN service configuration using a sequence of configuration forms and steps. To create a VPRN service, choose a subscriber from the Service Management→Manage Subscribers/Services form and configure the VPRN service for the chosen subscriber. Figure 26-1 shows the Create Service form with the Define Service Type parameters displayed and VPRN chosen as the service type.

Figure 26-1 VPRN main service creation - Define Service Type form

The screenshot shows a web-based configuration interface. On the left, a 'Steps' sidebar lists five steps: 1. Define Service Type (highlighted in blue), 2. Configure Sites, 3. L3 Interfaces Summary, 4. Configure Circuits, and 5. Circuits Summary. The main content area is titled 'Define Service Type' and contains the following fields and controls:

- Service ID: A text input field containing '0'.
- Auto-Assign ID: A checked checkbox.
- Service Name: An empty text input field.
- Description: An empty text input field.
- Type: A dropdown menu with 'VPRN' selected.

At the bottom of the form, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

VPRN services use BGP to exchange the VPRN routes among the PE routers that participate in the VPRN. This is done in a way which ensures that routes from different VPRN remain distinct and separate, even if two VPRNs have an overlapping address space. PE routers distribute routes from between 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.

Each route within 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's VPRN, to the route which 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 a RD, which identifies the VPRN association. Thus the backbone core routers do not need to know the VPRN routes.

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 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:

- physical Ethernet port or POS port and channel
- encapsulation type
- encapsulation identifier (if required)

Table 26-1 describes the general functions performed by PE, P, and CE routers in a VPRN. See Figure 26-2 in this chapter for a sample VPRN. See the *7750 SR OS Services Guide* for more detailed information about VPRN functionality on the 7750 SR.

Table 26-1 VPRN router functionality

Router type	Functionality
PE	<ul style="list-style-type: none"> • Directly connected to PE, CE, and P routers • Learn VPRN routes from CE devices using e-BGP, RIP, or static routes • Maintain a separate routing table, called a VRF, for each service • Exchange VPRN route information with other PE routers 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 which 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
P	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Are directly connected to PE routers • Provide customer access to the VPRN

Policies

Common to all 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 and circuits, when the service is configured or modified. The following policies are common to all 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 Manager and the Access Egress Policy Manager.
- Scheduling policies define hierarchical rate limiting and scheduling to manage the scheduling of queues. Scheduler policies are configured using the Scheduler Policy Manager.
- Filter policies control network traffic into or out of an interface or circuit based on IP matching criteria. Filter policies are configured using the ACL IP Filter Manager.
- 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.
- Accounting policies count the traffic on a service to ensure proper billing and enforcement of SLAs. Accounting policies are configured using the Accounting Policy Manager.

See chapter 20 for more information about policies.

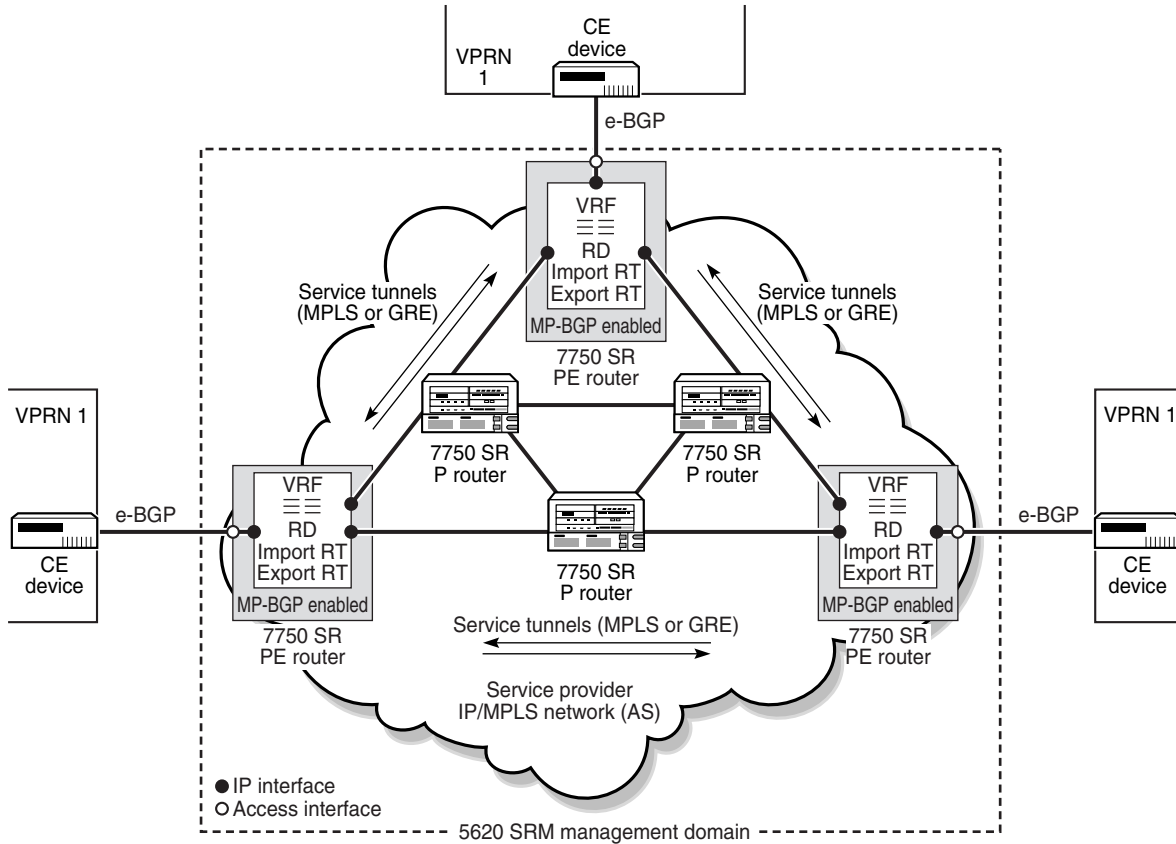
Troubleshooting

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 29 for more information.

26.2 Sample VPRN configuration

Figure 26-2 shows a sample VPRN service configuration. Your configuration will vary depending on your network requirements.

Figure 26-2 Sample VPRN



17333

Assuming the core IP/MPLS or GRE network has already been configured, Table 26-2 lists the high-level tasks that are required to configure this sample VPRN service.

Table 26-2 Sample VPRN service configuration

Task	Description
1. Configure policies as required	<p>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.</p> <ul style="list-style-type: none"> • Routing policies. Choose Policies→Routing Policy Manager to open the routing policy form. • Access ingress and egress interface policies. Choose Policies→Access Ingress Policy or Policies→Access Egress Policy to open these forms. • Scheduler policy. Choose Policies→Scheduler Policy Manager to open the scheduler policy form. • ACL IP filter policies. These policies specify access control lists based on IP addresses. Choose Policies→Acl IP Filter Manager to open the ACL form. • Accounting policy. Choose Policies→Accounting Policy to open the accounting policy form.
2. Configure ports as access ports for use in the service	<p>Right click on a port from the equipment navigation tree and choose Properties. Specify the port as an access port and specify an encapsulation type, if required.</p>

(1 of 2)

Task	Description
3. Configure service tunnels as required	Choose Topology→Service Tunnel Manager 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 17 for more information about protocol configuration. <ul style="list-style-type: none"> • Right click on a router instance from the network navigation tree and choose Properties. In the Properties form that appears, click on the Protocols tab and select the BGP check mark box. • Right click on the BGP instance from the network navigation tree and choose Properties. In the Properties form that appears, click on the VPN tab and select the VPN IPv4 check mark box. • Right click on the BGP Peer Group instance and choose Create Peer. In the Peer form that appears, configure the Peer Address and other parameters as required.
5. Create and configure subscribers	Choose Service Management→Manage Subscribers/Services to open the subscriber manager form and create a subscriber.
6. Create and configure the Service	Click on the Services tab on the subscriber manager form and click on the Add button to create a service. A series of steps, substeps, and forms guide the user through the service creation process. Configure the following key elements when to configure the service. <ul style="list-style-type: none"> • Specify a customer as the subscriber for the VPRN service. • Define the service type as VPRN. • Specify and configure the routers (sites) for the subscriber's VPRN service. For each VRF: <ul style="list-style-type: none"> • Configure autobinding, which specifies if the service that you are creating will be 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. • If required, configure static routes, BGP, or RIP on PE routers for PE to CE routing. • Configure and specify access interfaces on each of the routers for the VPRN service. <ul style="list-style-type: none"> • Configure a name, ID, MAC address, and other parameters. • Specify the ports for the access interfaces. Ports must be configured as access ports. • Specify participation of the access interfaces in ingress and egress policies, as required. • Specify if the access interfaces will participate in aggregation rate limiting across a card or port. If aggregation is not required, specify the participation of access interfaces in ingress and egress scheduler policies. If aggregation is required, specify the participation of access interfaces in an aggregation scheduler policy. • Specify the participation of the access interfaces access in ACL filter policies as required. • Specify the participation of the access interfaces access in accounting policies as required. • Specify ICMP parameters. • Specify the ARP timeout.
7. Create, update, or configure additional subscribers to the VPRN, or create a new VPRN with new or additional subscribers	Repeat the above tasks as required.

(2 of 2)

26.3 Workflow to create a VPRN service

- 1 Set up group and user access privileges.

- 2 Configure equipment and the network, including:
 - i Build the IP or IP/MPLS core network.
 - ii Create service tunnels, if required.
 - iii Configure ports for the service as access ports.
- 3 Configure pre-defined routing, QoS, scheduling, filter, and accounting policies. You do not have to create pre-defined policies if policies are created on a per-service basis.
- 4 Provision the service:
 - i Set up subscribers or associate existing subscribers with the new service.
 - ii Create the VPRN and associate the subscriber with the VPRN.
- 5 Turn up the service.

26.4 VPRN service management menus

Table 26-3 lists and describes the VPRN management menus.

Table 26-3 VPRN management menus

Menu item	Description
Service Management→Manage Subscribers/Services	Create subscribers and add or create services.
Service Management→Create Service	Create a service.
Service Management→Browse Services	Perform a filtered search on services.

26.5 VPRN service management procedures list

Table 26-4 lists the procedures necessary to perform VPRN service management tasks.

Table 26-4 VPRN management procedures list

Procedure	Purpose
To create a VPRN service	Create a VPRN service
To modify a VPRN	Modify a VPRN service
To delete a VPRN	Delete a VPRN service
To view the service topology	View a graphical representation of a VPRN service that shows the sites and interfaces.

26.6 VPRN service management procedures

Use the following procedures to perform VPRN creation and management tasks. See the *7750 SR OS Services Guide* for more information about VPRN configuration and parameters.

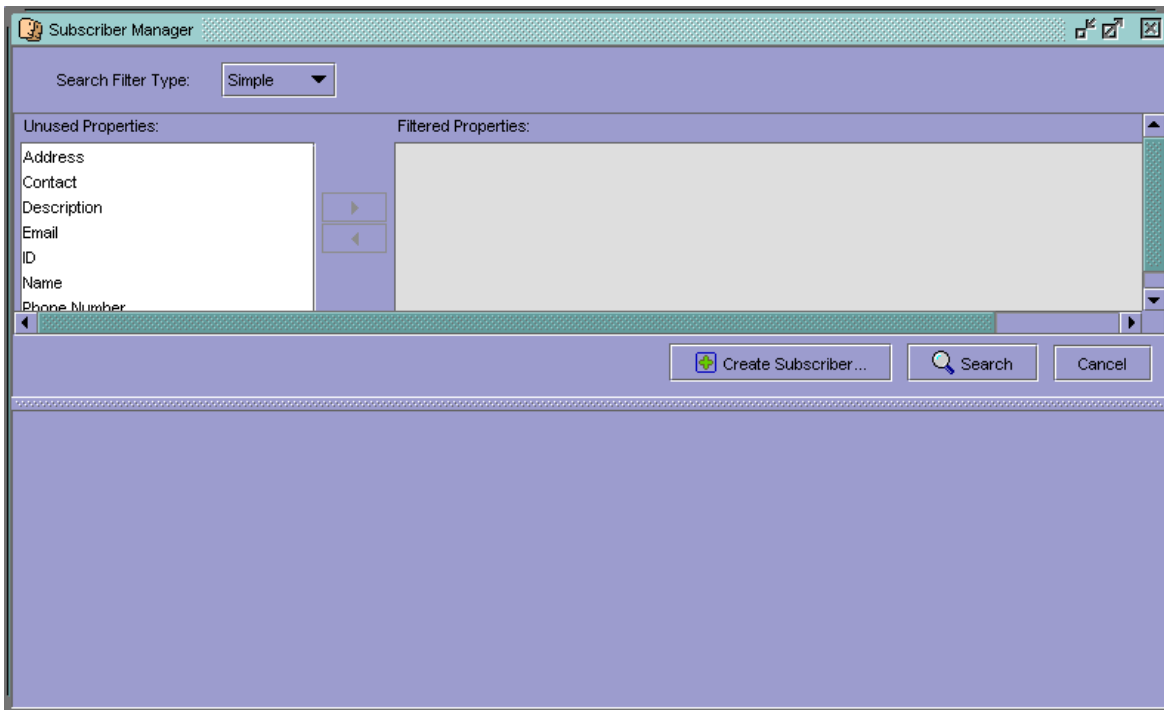
Procedure 26-1 To create a VPRN service

This procedure describes how to create a VPRN service using the Subscriber Manager form as the starting point. This allows you to browse a list of subscribers, and choose a subscriber for the service before you start creating the service.

You can also create a VPRN service using the Create Service form as the starting point. This allows you to choose a subscriber for the service during service configuration. Choose Service Management→Create Service from the 5620 SAM main menu.

- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu. The Subscriber Manager form opens as shown in Figure 26-3.

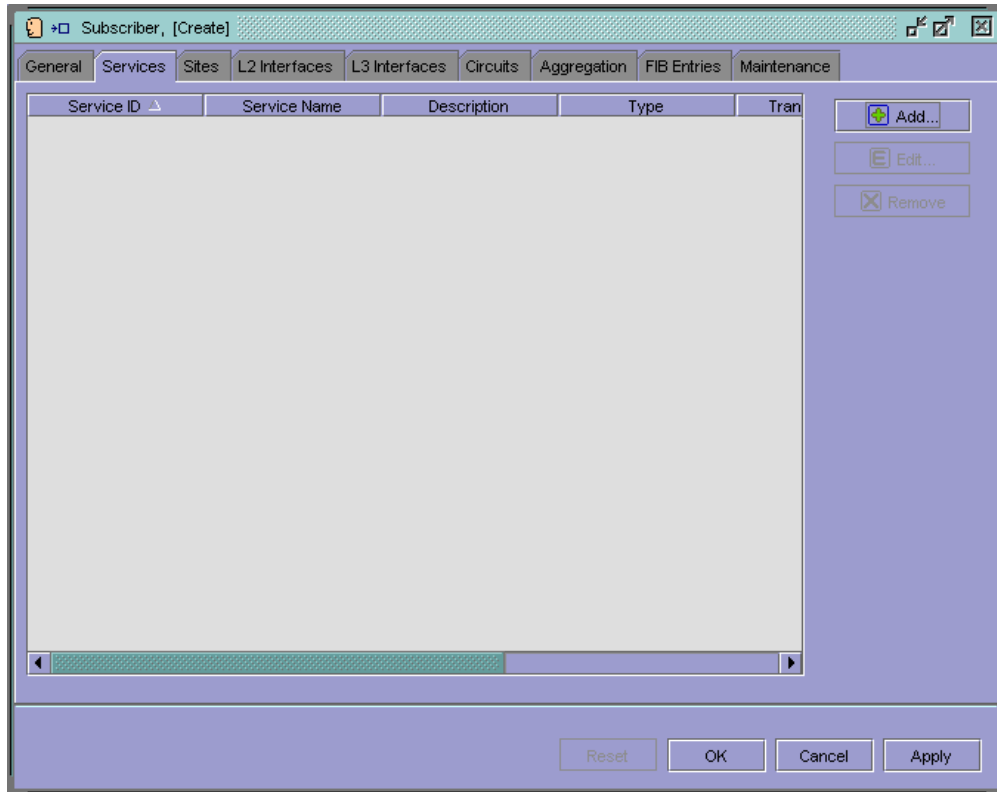
Figure 26-3 Subscriber Manager form



- 2 Configure the subscriber list filter parameters and click on the Search button. A list of available subscribers appears at the bottom of the Subscriber Manager form.
- 3 Choose a subscriber from the list to use the VPRN you are creating.
- 4 Click on the Edit button. The Subscriber form with the General tab opens.

- 5 Click on the Services tab. Figure 26-4 shows the Subscriber form with the Services tab button selected.

Figure 26-4 Subscriber form - Services



- 6 Click on the Add button. The Create Service - Define Service Type form opens, with VPLS chosen as the default service type, as shown in Figure 26-5.

Figure 26-5 Create Service - Define Service Type form

The screenshot shows a web-based form titled "Create Service - Define Service Type". On the left, a "Steps" sidebar lists six steps, with "1. Define Service Type" selected. The main form area contains the following fields:

- Service ID:** A text input field containing the value "0". To its right is a checked checkbox labeled "Auto-Assign ID".
- Service Name:** An empty text input field.
- Description:** An empty text input field.
- Type:** A dropdown menu currently showing "VPLS".

At the bottom of the form, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Configure the parameters.

- i** Specify how you want service IDs assigned. The ID uniquely identifies the service in the service domain.
 - To have the 5620 SAM automatically assign a service ID, select the Auto-Assign ID check box.
 - To manually assign a service ID, deselect the Auto-Assign ID check box. Configure the Service ID parameter. The range is 1 to 2 147 483 647
- ii** Configure the Service Name parameter. The name can be up to 32 characters.
- iii** Configure the service Description parameter. The description can be up to 80 characters.
- iv** Choose VPRN for the Type parameter. The series of steps to create the VPRN service appears, as shown in Figure 26-6.

Figure 26-6 Create Service - Define Service Type form

Steps

1. Define Service Type
2. Configure Sites
3. L3 Interfaces Summary
4. Configure Circuits
5. Circuits Summary

Define Service Type

Service ID: Auto-Assign ID

Service Name:

Description:

Type:

< Back Next > Finish Cancel

- 7 Click on the Next button. The Create Service - Configure Sites form opens.
- 8 Click on the Add button. The Create Service Site - Number of Sites form opens, as shown in Figure 26-7.

Choose Single from the drop-down menu.

Figure 26-7 Create Service Site - Number of Sites form

Steps

1. Number of Sites
2. Select Site
3. Define General Properties
4. Configure Auto-Bind
5. Define Routing Properties
6. Configure VRF Target
7. Configure Import Policies
8. Configure Export Policies
9. Configure L3 Interfaces
10. Configure Static Routes
11. Configure Protocols

Number of Sites

How many sites would you like to add in this step?

Single ▼

< Back Next > Finish Cancel

- 9 Click on the Next button. The Create Service Site - Select Site form opens.
Click on the Select button to list and choose a site.
- 10 Click on the Next button. The Create Service Site - Define General Properties form opens.
Configure the parameters.
 - i Configure the site Description parameter. The description can be up to 80 characters.
 - ii Configure the site Administrative State parameter. The options are Up or Down.
- 11 Click on the Next button. The Create Service Site - Configure Auto-Bind form opens.
Configure the Transport parameter. Auto-bind specifies whether the service you are creating will be automatically bound to previously created service tunnels. The options are None, MPLS:LDP, or GRE.
 - a Specify None if you want to explicitly specify service tunnels and circuits for the service in step 44 of this procedure.

- b Specify MPLS:LDP if you want the service to be automatically bound to MPLS service tunnels. You do not have to specify service tunnels and circuits for the service in step 44 of this procedure.



Note — To use MPLS as the transport type, you must bind LSPs to service tunnels during service tunnel configuration. See Procedure 19-1 for more information.

- c Specify GRE if you want the service to be automatically bound to GRE service tunnels in step 44 of this procedure.
- 12 Click the Next button. The Create Service Site - Define Routing Properties form opens, as shown in Figure 26-8.

Figure 26-8 Create Service Site - Define Routing Properties form

Steps

1. Number of Sites
2. Select Site
3. Define General Properties
4. Configure Auto-Bind
5. Define Routing Properties
6. Configure VRF Target
7. Configure Import Policies
8. Configure Export Policies
9. Configure L3 Interfaces
10. Configure Static Routes
11. Configure Protocols

Define Routing Properties

Router ID:

Maximum Number Of Equal Cost Routes:

Autonomous System:

Enforce Maximum Number Of Routes:

Route Distinguisher Type:

< Back Next > Finish Cancel

Configure the parameters.

- i** Specify the router id for the VRF for the Router ID parameter.
 - ii** Configure the Maximum Number of Equal Cost Routes parameter. The range is 0 to 16.
 - iii** Configure the Autonomous System parameter to specify the customer edge to provider edge AS. This defines the AS to be used by the VRF table on this provider edge device. The range is 0 to 65 535.
 - iv** Select the Enforce Maximum Number of Equal Cost Routes parameter if you want to enforce the maximum number of routes. If you select the parameter, you must also perform step 13 of this procedure.
 - v** Specify a type for the Route Distinguisher Type parameter.
 - Specify None if you do not want to specify a route distinguisher. Go to step 16 of this procedure.
 - Specify Type 0 if you want to specify an AS number for the route distinguisher. Go to step 14 of this procedure.
 - Specify Type 1 if you want to specify an IP address for the route distinguisher. Go to step 15 of this procedure.
- 13** Click on the Next button. The Create Service Site - Configure Maximum Routes form opens. Configure the parameters.
 - i** Specify a value for the Maximum Number of Routes parameter. This is the maximum number of routes within the VRF. The range is 0 to 2 147 483 647.
 - ii** Specify the Log Only parameter. This determines whether an SNMP trap is sent when the maximum number of routes is exceeded, or whether the BGP or RIP peer is disabled while keeping the VPRN instance enabled. The options are true or false.
 - iii** Specify the Threshold (%) parameter. This determines the threshold at which to send logs and SNMP traps when the maximum number of routes threshold is almost reached. The range is 0 to 100.
- 14** Click on the Next button. The Create Service Site - Configure Type 0 Route Distinguisher form opens. Configure the parameters.
 - i** Configure the Type 0 Administrative Value parameter. This is the AS number for the RD. The range is 1 to 65 535.

You can set the AS number to 0 when you use static routing or RIP between the PE and CE routers. The AS number can also be the AS of the PE router (base router instance). Alcatel recommends that you do not use private AS numbers.
 - ii** Configure the Type 0 Assigned Value parameter. The range is 0 to 4 294 967 295.

Go to step 16 of this procedure.

- 15 Click on the Next button. The Create Service Site - Configure Type 1 Route Distinguisher form opens. Configure the parameters.
 - i Specify an IP address for the Type 1 IP Address parameter. Alcatel recommends that you do not use private IP address spaces.
 - ii Configure the Type 1 Assigned Value parameter. The range is 1 to 65 535.
- 16 Click on the Next button. The Create Service Site - Configure VRF Target form opens, as shown in Figure 26-9.

Figure 26-9 Create Service Site - Configure VRF Target form

Route targets are used to identify the VRFs of a VPRN. A PE router (which is not a route reflector or an AS border router) will install a VPRN route only when its import target matches the target of the route.

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 all 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.

Configure the VRF Target Type parameter. The options are None, Define Default, or Define Import and Export.

- a Specify None if you do not want to specify a VRF target for the site. Go to step 22 of this procedure.
- b Specify Define Default if you want to specify a default VRF target for the site. Go to step 17 of this procedure.

Figure 26-10 shows the Configure Import and Export Target form with AS specified as the import target format and IP address specified as the export target format. Note the 5620 SAM steps to configure the AS-Based Import Target and the IP Address-Based Export Target.

Figure 26-10 Configure Import and Export Targets form

21 Click on the Next button to go to the next 5620 SAM step. Configure the parameters.

- a** When the Create Service Site - Configure AS-Based Import Target form opens.
 - i** Specify a value for the Import Target AS Value parameter. The range is 1 to 65 535.
 - ii** Specify a value for the Import Target Extended Community Value parameter. The range is 0 to 4 294 967 295.

Click on the Next button to go to the next 5620 SAM step.

- b** When the Create Service Site - Configure AS-Based Export Target form opens.
 - i** Specify a value for the Export Target AS Value parameter. The range is 1 to 65 535.
 - ii** Specify a value for the Export Target Extended Community Value parameter. The range is 0 to 4 294 967 295.

Click on the Next button to go to the next 5620 SAM step.

- c When the Create Service Site - Configure IP Address-Based Import Target form opens.
 - i Specify an IP address for the Import Target IP Address parameter.
 - ii Specify a value for the Import Target Community Value parameter. The range is 0 to 65 535.

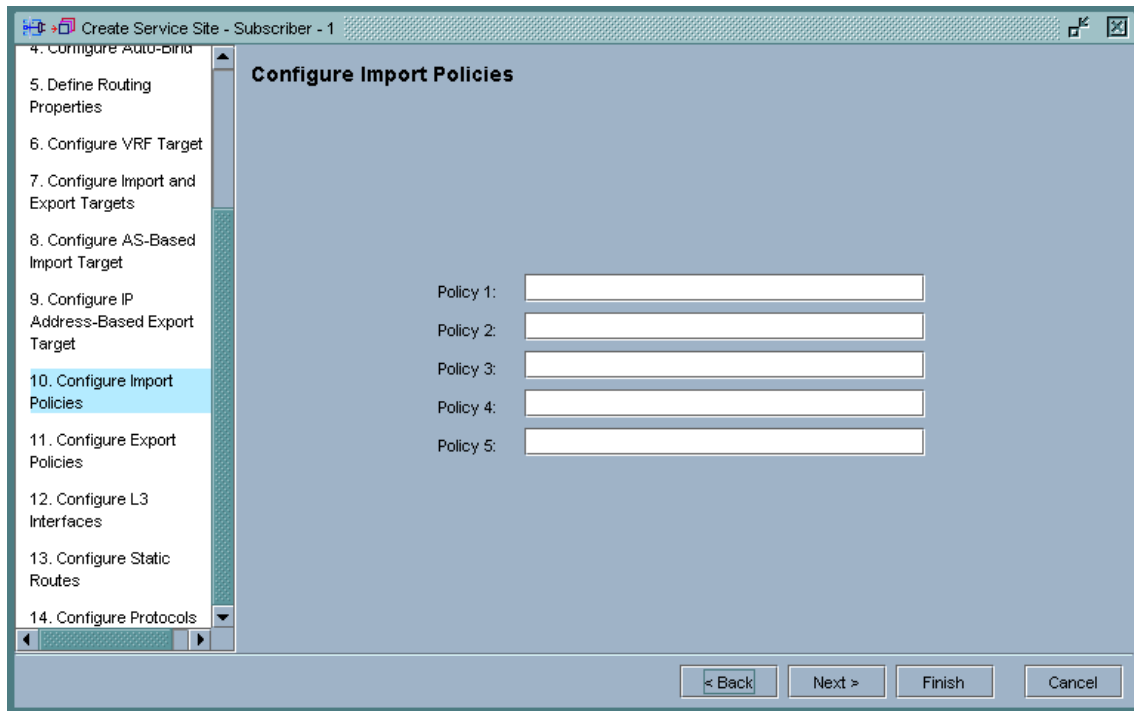
Click on the Next button to go to the next 5620 SAM step.

- d When the Create Service Site - Configure IP Address-Based Export Target form opens.
 - i Specify an IP address for the Export Target IP Address parameter.
 - ii Specify a value for the Export Target Community Value parameter. The range is 0 to 65 535.

Click on the Next button to go to the next 5620 SAM step.

- 22 Click on the Next button. The Create Service Site - Configure Import Policies form opens, as shown in Figure 26-11.

Figure 26-11 Configure Import Policies form



Specify the import route policies to be used. You can specify up to five policies.

- 23 Click on the Next button. The Create Service Site - Configure Export Policies form opens.

Specify the export route policies to be used. You can specify up to five policies.

- 24 Click on the Next button. The Create Service Site - Configure L3 Interfaces form opens, as shown in Figure 26-12.

Figure 26-12 Create Service Site - Configure L3 Interfaces form

The screenshot shows a software window titled "Create Service Site - Subscriber - 2". On the left is a vertical navigation pane with a list of steps: 4. Configure Auto-Bind, 5. Define Routing Properties, 6. Configure Type 0 Route Distinguisher, 7. Configure VRF Target, 8. Configure Import and Export Targets, 9. Configure AS-Based Import Target, 10. Configure Import Policies, 11. Configure Export Policies, 12. Configure L3 Interfaces (highlighted in blue), 13. Configure Static Routes, and 14. Configure Protocols. The main content area is titled "Configure L3 Interfaces" and features a table with the following headers: "Service ID", "Service Name", "Service Type", and "Site ID". The table body is currently empty. To the right of the table are three buttons: "Add..." (with a plus icon), "Edit..." (with an edit icon), and "Remove" (with a minus icon). At the bottom of the window are four buttons: "< Back", "Next >", "Finish", and "Cancel".

- 25 Click on the Add button. The Create L3 Interface - Define General Properties form opens, as shown in Figure 26-13.

Figure 26-13 Create L3 Interface - Define General Properties form

Configure the parameters.

- i Specify how you want interface IDs assigned. The ID uniquely identifies the interface in the service domain.
 - To have the 5620 SAM automatically assign an interface ID, select the Auto-Assign ID check box.
 - To manually assign an interface ID, deselect the Auto-Assign ID check box. Configure the Interface ID parameter. The range is 2 to 5119.
 - ii Configure the interface Name parameter. The name can be up to 32 characters.
 - iii Configure the interface Description parameter. The description can be up to 80 characters.
 - iv Configure the interface Administrative State parameter. The options are Up or Down.
 - v Specify a MAC address for the interface for the MAC Address parameter.
 - vi Select the Allow Direct Broadcasts check box to enable the forwarding of direct broadcasts from the interface.
 - vii Select the Loopback Enabled check box to enable loopbacks on the interface.
- 26 Click on the Next button. The Create L3 Interface - Configure IP Address form opens.
 - 27 Click on the Add button. The IP Address form opens as shown in Figure 26-14.

Figure 26-14 IP Address form

Configure the parameters.

- i Specify an interface IP address for the IP Address parameter. You can choose one primary IP address for the IP interface
- ii Specify a mask for the Subnet Mask parameter.
- iii Specify a format for the Broadcast Address Format parameter. The options are All Ones or Host Ones.
- iv Select the Primary check box if you want the IP address to be the primary IP address for the interface.

After you assign a primary IP address to the interface, you can assign multiple secondary IP addresses to the interface. Repeat this step and deselect the Primary check box to assign additional IP addresses to the interface.

- 28 Click on the OK button. The IP Address form closes and the Create L3 Interface - Configure IP Address form re-opens. The IP address and other parameters are displayed in the form.
- 29 Click on the Next button. The Create L3 Interface - Select Port form opens, as shown in Figure 26-15.

Figure 26-15 Create L3 Interface - Select Port form

Steps

1. Define General Properties
2. Configure IP Address
3. Select Port
4. Configure ICMP
5. Configure ARP

Select Port

Port:

Port ID:

Encap Type:

Outer Encapsulation Value: Inner Encapsulation Value:

< Back Next > Finish Cancel

Configure the parameters.

- i Click on the Select button to list and choose a port or channel.

You can only choose ports or channels in access mode. Use the 5620 SAM navigation tree to choose a port or channel and set the Mode parameter to Access.

After you choose a port or channel, additional steps to configure the interface appear, as shown in Figure 26-16.

Figure 26-16 Create L3 Interface - Select Port form

- ii Configure the Inner Encapsulation Value and the Outer Encapsulation Value parameters.

One or both parameters are configurable when the port encapsulation type is Dot1q, Q in Q, BCP Dot 1q, or FR. Use the 5620 SAM navigation tree to choose a port or channel and specify an option for the port Encap Type parameter.

The range for the Inner Encapsulation Value and the Outer Encapsulation Value parameters depend on the option you choose for the port Encap Type parameter.

- 30 Click on the Next button. The Create L3 Interface - Select QoS Policies form opens, as shown in Figure 26-17.

Figure 26-17 Create L3 Interface - Select QoS Policies form

- i Click on the Ingress: Select button to list and choose an access ingress policy.
 - ii Click on the Egress: Select button to list and choose an access egress policy.
- 31** Click on the Next button. The Create L3 Interface - Aggregation form opens.

Configure the Aggregation parameter. The parameter specifies whether an aggregation scheduler policy will be applied to the interface. The options are On or Off.

When you choose On, go to step 32 of this procedure.

When you choose Off, go to step 33 of this procedure.

- 32** Click on the Next button. The Create L3 Interface - Select Aggregation Scheduler Policy form opens.

Click on the Select button to list and choose an aggregation scheduler policy.

Go to step 34 of this procedure.

- 33** Click on the Next button. The Create L3 Interface - Select Ingress and Egress Scheduler Policies form opens
- i Click on the Ingress: Select button to list and choose an ingress scheduler policy.
 - ii Click on the Egress: Select button to list and choose an egress scheduler policy.

- 34** Click on the Next button. The Create L3 Interface - Select ACL Filters form opens.
- i** Click on the Ingress: Select button to list and choose an ingress ACL filter.
 - ii** Click on the Egress: Select button to list and choose an egress ACL filter.
- 35** Click on the Next button. The Create L3 Interface - Select Accounting Policy form opens.
- Configure the parameters.
- i** Click on the Select button to list and choose an accounting policy.
 - ii** Select the Accounting Enabled check box to enable the collection of accounting statistics for the interface.
- 36** Click on the Next button. The Configure ICMP form opens, as shown in Figure 26-18.

Figure 26-18 Configure ICMP form

The screenshot shows a web browser window titled "Create L3 Interface - 10.1.1.18, Subscriber - 1". The main content area is titled "Configure ICMP". On the left, a "Steps" sidebar lists 10 steps, with "9. Configure ICMP" highlighted. The main area contains the following configuration options:

Mask Reply:	<input checked="" type="checkbox"/>		
Redirects:	<input checked="" type="checkbox"/>		
Number of Redirects:	<input type="text" value="100"/>	Redirects Time (seconds):	<input type="text" value="10"/>
Unreachables:	<input checked="" type="checkbox"/>		
Number of Unreachables:	<input type="text" value="100"/>	Unreachables Time (seconds):	<input type="text" value="10"/>
TTL Expired:	<input checked="" type="checkbox"/>		
Number of TTL Expired:	<input type="text" value="100"/>	TTL Expired Time (seconds):	<input type="text" value="10"/>

At the bottom of the form are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Configure the parameters.

- i Select the Mask Reply check box to enable responses to the ICMP mask requests on the router interface.
 - ii Select the Redirects check box to enable configuration of rates for ICMP redirect messages on the router interface. Redirects are issued by the router when the router determines that a more optimal route is available.
 - iii Configure the Number of Redirects parameter. The range is 10 to 1000.
 - iv Configure the Redirects Time (seconds) parameter. The range is 1 to 60.
 - v Select the Unreachables check box to enable the configuration of the rate for ICMP host and network destination unreachable messages issued on the router interface.
 - vi Configure the Number of Unreachables parameter. The range is 10 to 1000.
 - vii Configure the Unreachables Time (seconds) parameter. The range is 1 to 60.
 - viii Select the TTL Expired check box to enable the rate of ICMP TTL expired messages issued by the router interface.
 - ix Configure the Number of TTL Expired parameter. The range is 10 to 1000.
 - x Configure the TTL Expired Time (seconds) parameter. The range is 1 to 60.
- 37** Click on the Next button. The Create L3 Interface - Configure ARP form opens, as shown in Figure 26-19.

Figure 26-19 Create L3 Interface - Configure ARP form

The screenshot shows a web-based configuration interface. The title bar reads "Create L3 Interface - 10.1.1.214, Subscriber - 2". On the left side, there is a "Steps" sidebar with a list of 10 steps. Step 10, "Configure ARP", is highlighted in blue. The main content area is titled "Configure ARP" and features a "Timeout:" label with a text input field containing the value "14400". At the bottom of the form, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Configure the ARP Timeout parameter. The parameter specifies, in seconds, how long an ARP entry is maintained without being refreshed. The range is 0 to 65 535.

- 38 Click on the Finish button. The Create L3 Interface - Configure ARP form closes and the Create Service Site - Configure L3 Interfaces form re-opens. The interface and interface parameters are listed in the form.

You can add, edit, or remove interfaces.

- 39 Click on the Next button. The Create Service Site - Configure Static Routes form opens.
- 40 Click on the Add button. The Static Route form opens, as shown in Figure 26-20.

Figure 26-20 Configure Static Routes form

The screenshot shows the 'Configure Static Routes' form with the following details:

- Title:** Configure Static Routes
- Table:**

Static Route ID	Routing Instance ID	Routing Instance Name	Destination
0	1		
- Buttons:** Add..., Edit..., Remove
- Form Fields:**
 - Static Route ID: 0
 - Auto-Assign ID:
 - Routing Instance ID: 1
 - Routing Instance Name: (empty)
 - Destination: (empty)
 - Mask: (empty)
 - Type: Next Hop
 - IP Address: 0.0.0.0
 - Preference: 5
 - Metric: 1
 - Administrative State: Up
 - Operational State: Down
- Bottom Buttons:** Reset, OK, Cancel, Apply
- Navigation Buttons:** < Back, Next >, Finish, Cancel

If static routes are required, configure the parameters to define the static routes that will be exchanged with the CE from the PE VRF.

- i** Specify how you want static route IDs assigned. The ID uniquely identifies the static route in the service domain.
 - To have the 5620 SAM automatically assign a static route ID, select the Auto-Assign ID check box.
 - To manually assign a static route ID, deselect the Auto-Assign ID check box.
Enter a value for the Static Route ID parameter. The range is 1 to 2 147 483 647
 - ii** Specify a destination IP address for the Destination parameter.
 - iii** Specify a destination mask for the Mask parameter.
 - iv** Configure the hop Type parameter. The options are Next Hop, Indirect, or Black Hole.
 - v** Specify the next hop or indirect IP address for the IP Address parameter.
 - vi** Configure the Preference parameter. The range is 1 to 256.
 - vii** Configure the Metric parameter. The range is 0 to 65 535.
 - viii** Configure the static route Administrative State parameter. The options are Up or Down.
 - ix** Click on the OK button. The Static Route configuration form closes and the Create Service Site - Configure Static Routes re-opens. The static route and route parameters appear in the form.
- 41** Click on the Next button. The Create Service Site - Configure Protocols form opens, as shown in Figure 26-21.

Figure 26-21 Create Service Site - Configure Protocols form

Configure Protocols

BGP Enabled:

RIP Enabled:

Site Name	Site ID	Name	Administrative State
-----------	---------	------	----------------------

Buttons: < Back, Next >, Finish, Cancel

Configure the parameters.

- i If required, select the BGP Enabled check mark box to enable BGP for PE to CE routing.
- ii If required, select the RIP Enabled check mark box to enable RIP for PE to CE routing.

When you select a protocol, the router and the protocol enabled on the router appear in the list panel.

- 42** Click on the Finish button. The Create Service Site - Configure Protocols form closes and the Create Service - Configure Sites form re-opens. The site and the site parameters are listed.

You can add, edit, or remove sites.

- 43** Click on the Next button. The Create Service - L3 Interfaces Summary form opens, as shown in Figure 26-22.

Figure 26-22 Create Service - L3 Interfaces Summary form

Service ID ▾	Service Name	Service Type	Site ID
0	VPRN		10.1.1.214

Interface and interface parameters are listed. You can add, edit, or remove interfaces.

- 44 Click on the Next button. The Create Service - Configure Circuits form opens, as shown in Figure 26-23.

Figure 26-23 Create Service - Configure Circuits form

Steps

1. Select Subscriber
2. Define Service Type
3. Configure Sites
4. L3 Interfaces Summary
5. Configure Circuits
6. Circuits Summary

Configure Circuits

Bidirectional

From:

Site ID	Site Name	Description
10.1.1.18	pc18	

To:

Site ID	Site Name
10.1.1.18	pc18

Circuit:

Tunnel ID	Tunnel Name	Type	Transport
-----------	-------------	------	-----------

Add... Edit... Remove

< Back Next > Finish Cancel

- If you chose MPLS:LDP or GRE for the Transport parameter in the Configure Auto-Bind form in step 11 of this procedure, you do not have to configure circuits. Click on the Finish button and go to step 52 of this procedure.
 - If you chose None for the Transport parameter in the Configure Auto-Bind form in step 11 of this procedure, you must configure circuits. Go to step 45 of this procedure.
- 45** In the Create Service - Configure Circuits form, click on the Add button. The Create Circuit - Select Source Node form appears as shown in Figure 26-24. Choose a source node.

Figure 26-24 Create Circuit - Select Source Node form

Site ID	Site Name	Description	Admin
10.1.1.18	pc18		Up
10.1.1.214	pc214		Up

Source Node ID: Source Node Name:

< Back Next > Finish Cancel

- 46 Click on the Next button. The Create Circuit - Select Destination Node form opens.
Choose a destination node.
- 47 Click on the Next button. The Create Circuit - Select Tunnel form opens.
Click on the Select button to list and choose a tunnel.
- 48 Click on the Next button. The Create Circuit - Define General Properties form opens.
Configure the circuit Administrative State parameter. The options are Up or Down.
- 49 Click on the Finish button. The Create Circuit - Define General Properties form closes and the Create Service - Configure Circuits form re-opens.

You can list the circuits and circuit parameters in the circuit list that appears at the bottom of the form. Choose the Unidirectional or Bidirectional parameter and selecting routers from the To and/or From lists. The circuits that appear in the circuits list are filtered according to the criteria you specify.

You can add, edit, or remove circuits.
- 50 Click on the Next button. The Create Service - Circuits Summary form opens.
Circuits and circuit parameters are listed in the form.

You can add, edit, or remove circuits.
- 51 Click on the Finish button. The Create Service - Circuits Summary form closes and the Subscriber Manager form re-opens. The service and service parameters are listed in the form.

You can add, edit, or remove services.

- 52 Click on the Apply button to save the service.
-

Procedure 26-2 To modify a VPRN

- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu.
- 2 Configure the subscriber list filter parameters and click on the Search button. A list of available subscribers appears at the bottom of the Subscriber Manager form.
- 3 Choose a subscriber from the list.
- 4 Click on the Edit button. The Subscriber form with the General tab opens.
- 5 Click on the Services tab. A list of services appears.
- 6 Choose a service.
- 7 Click on the Edit button. A Service edit form with the General tab opens.
- 8 Modify the parameters for the service as required.



Caution — Modifying parameters can be service-affecting.

The parameter information that appears for the service includes:

- General tab that displays the general properties of the service
 - Sites tab that lists the sites included in the service
 - L3 Interface tab that lists interfaces used by the service
 - Addresses tab
 - Faults tab that displays faults associated with the service
- 9 Click on the OK button to close the Service edit form. The Subscriber form re-opens.
 - 10 Click on the Apply button to save the modified service.
-

Procedure 26-3 To delete a VPRN

- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu.
- 2 Configure the subscriber list filter parameters and click on the Search button. A list of available subscribers appears at the bottom of the Subscriber Manager form.
- 3 Choose a subscriber from the list.

- 4 Click on the Edit button. The Subscriber form with the General tab opens.
 - 5 Click on the Services tab. A list of services appears.
 - 6 Choose a service.
 - 7 Click on the Remove button. The service is removed from the list.
 - 8 Click on the Apply button to delete the service.
-

Procedure 26-4 To view the service topology

- 1 Choose Service Management→Manage Subscribers/Services from the 5620 SAM main menu.
 - 2 Configure the subscriber list filter parameters and click on the Search button. A list of available subscribers appears at the bottom of the Subscriber Manager form.
 - 3 Choose a subscriber from the list.
 - 4 Click on the Edit button. The Subscriber form with the General tab opens.
 - 5 Click on the Services tab. A list of services appears.
 - 6 Choose a service.
 - 7 Click on the Edit button. A Service edit form with the General tab opens.
 - 8 Click on the Topology view button. The service topology map opens.
See chapter 27 for more information about service topology views.
-

27 — Map management

- 27.1 Network topology maps overview 27-2**
- 27.2 Map management workflow 27-7**
- 27.3 Map menus 27-7**
- 27.4 Map management procedures list 27-7**
- 27.5 Map management procedures 27-8**

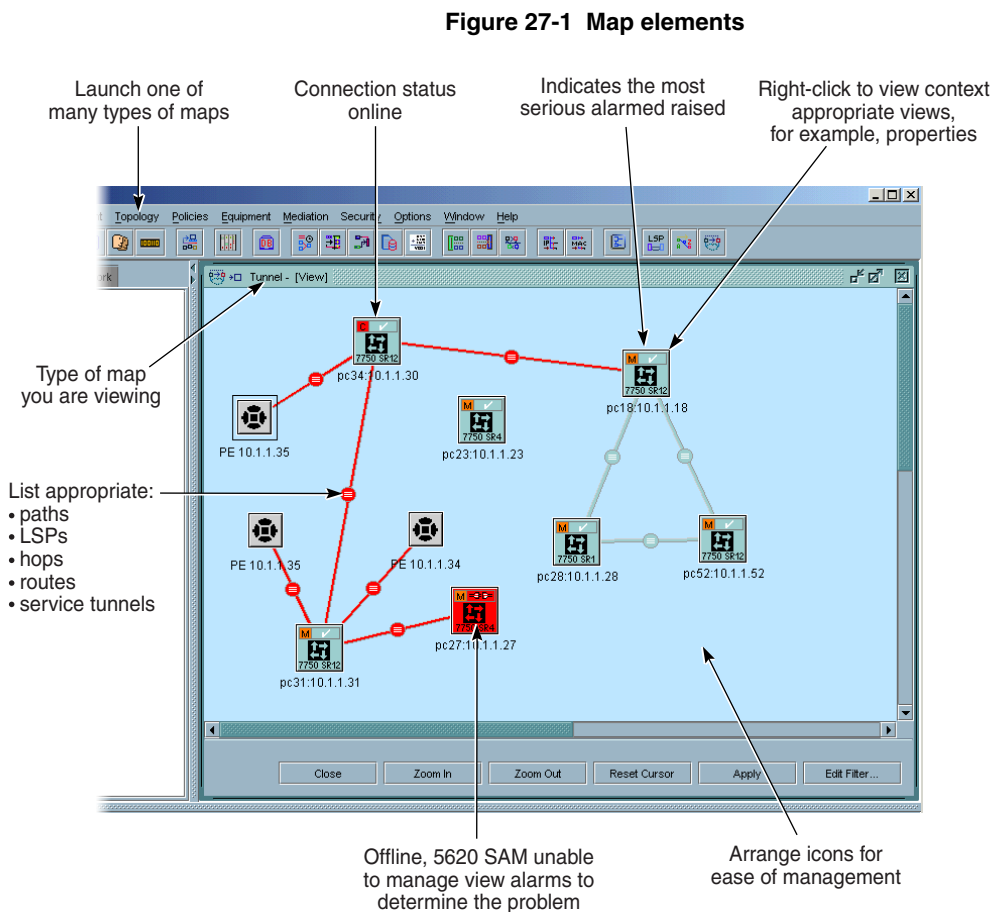
27.1 Network topology maps overview

The following network topology maps are available on the 5620 SAM:

- LSP topology map
- LSP path topology map
- service topology map
- service path topology maps

The maps visually display network information, and provide contextual menus and submenus to open forms which display additional information.

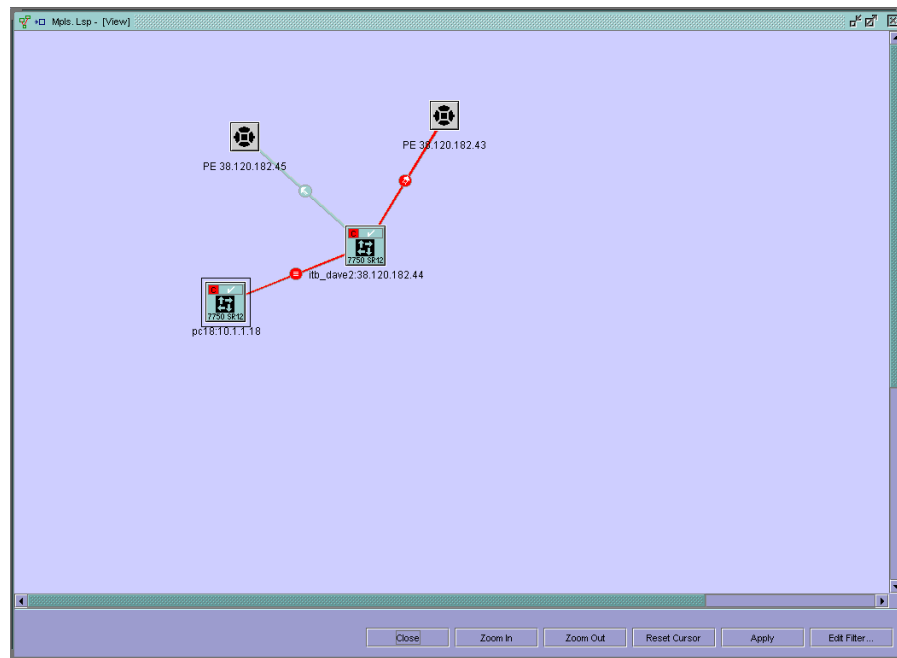
Figure 27-1 shows the main elements of a map.



17260

LSP topology map

An LSP topology map is available on the 5620 SAM by choosing Topology→LSP Topology from the 5620 SAM main menu. Configure the network filter parameters in the form that appears and click on the OK button. The LSP topology map appears as shown in Figure 27-2.

Figure 27-2 LSP topology map

The LSP topology map is used to view all LSPs in a grouped manner, according to their source and destination nodes.

When you view the LSP topology map, the source and destination devices are linked by straight lines, where each line represents the group of RSVP-TE LSPs between the two devices. When all the LSPs of the group are in the same direction, an arrow indicates the direction. When the LSPs are in different directions, a circle is shown.

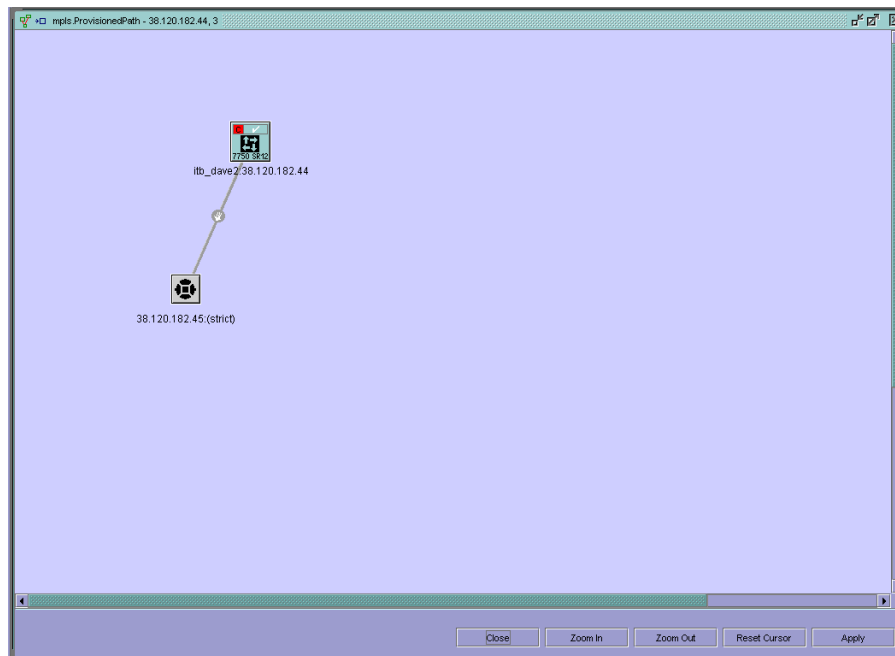
The LSP topology map includes:

- source and destination devices
- status of the device at the source and destination
- device type, name, and system identifier
- system IP addresses of non-managed devices

LSP path topology map

An LSP path topology map is available from the MPLS path manager form and the LSP Manager form. The LSP path topology map is used to view a specific provisioned or actual LSP path in the context of its source, and transient and destination hops. Figure 27-3 shows an LSP path topology map.

Figure 27-3 LSP path topology map



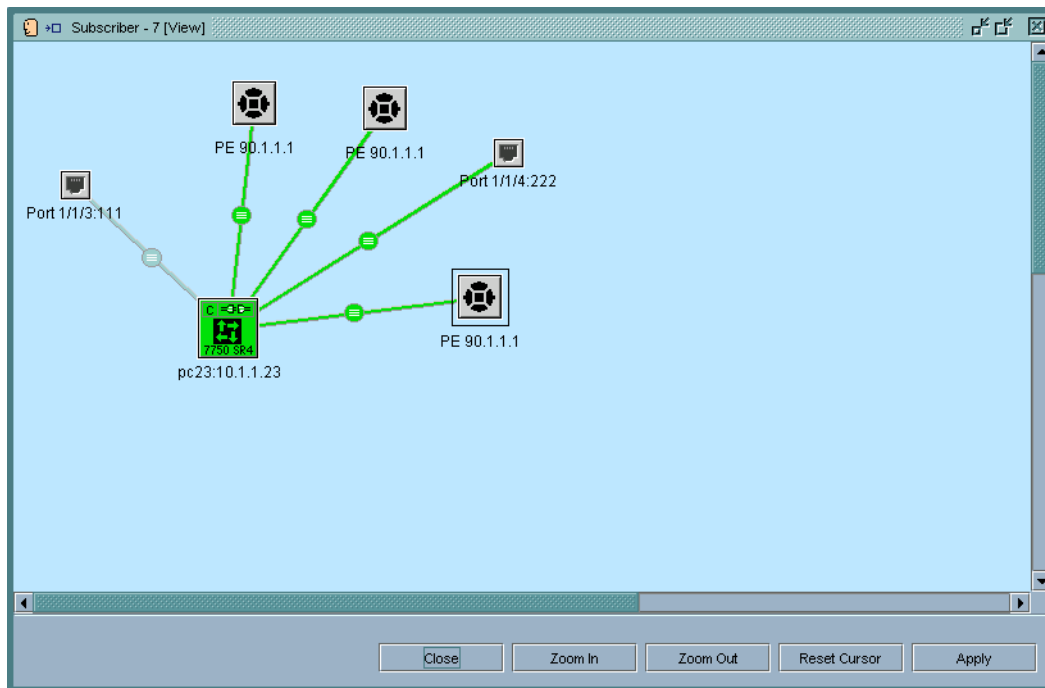
When you view the LSP path topology map, hops are linked by straight lines, where each line represents a sub-path between two hops of the LSP path. The direction of each path is indicated by an arrow. Green lines indicate provisioned paths, and gray lines indicate actual paths.

Service topology map

A service topology map view is available on the 5620 SAM from the Subscriber Manager form or from the Services configuration form.

To view the map from the Subscriber Manager form, choose Service Management→Manage Services/Subscribers from the 5620 SAM main menu. List and choose a subscriber or subscribers from the Subscriber Manager form that appears and click on the Topology View button. The subscriber service topology map appears, as shown in Figure 27-4.

Figure 27-4 Subscriber service map view



The large icons represent managed devices. Red indicates that one or more services on the device is down. Green indicates that all services are up. The small icons represent unmanaged devices. The port icons represent managed access interfaces.

The symbol and color in the top left corner of the managed device icon represents the most severe alarm on any of the services on the device. The symbol and color in the top right corner represents the most critical status of any of the services.

Right-click on a managed device to open a contextual menu which lists all services for the subscriber or subscribers on the device. Contextual submenus allow you to open additional information forms, including the Properties form for a service.

You can right click anywhere on the subscriber service map to open contextual menus and submenus for all services for the subscriber or subscribers. You can also right click on an access interface to open contextual menus and submenus for the interface.

Link groups between managed devices and access interfaces represent the binding of an access interface to a service. Link groups between devices represent service circuits. Right-click on the link group icon to open contextual menus and submenus. When you view the properties for a circuit, you can determine the type of circuit, for example, whether the circuit is a spoke into a service, or part of circuit mesh for the service.

To view the map from the Services tab in the Subscriber form, choose Service Management→Manage Services/Subscribers from the 5620 SAM main menu and list subscribers by clicking on the Search button. Double-click on a subscriber and click on the Services tab in the Subscriber form that appears. Double-click on a service and click on the Topology Map view button in the form that appears.

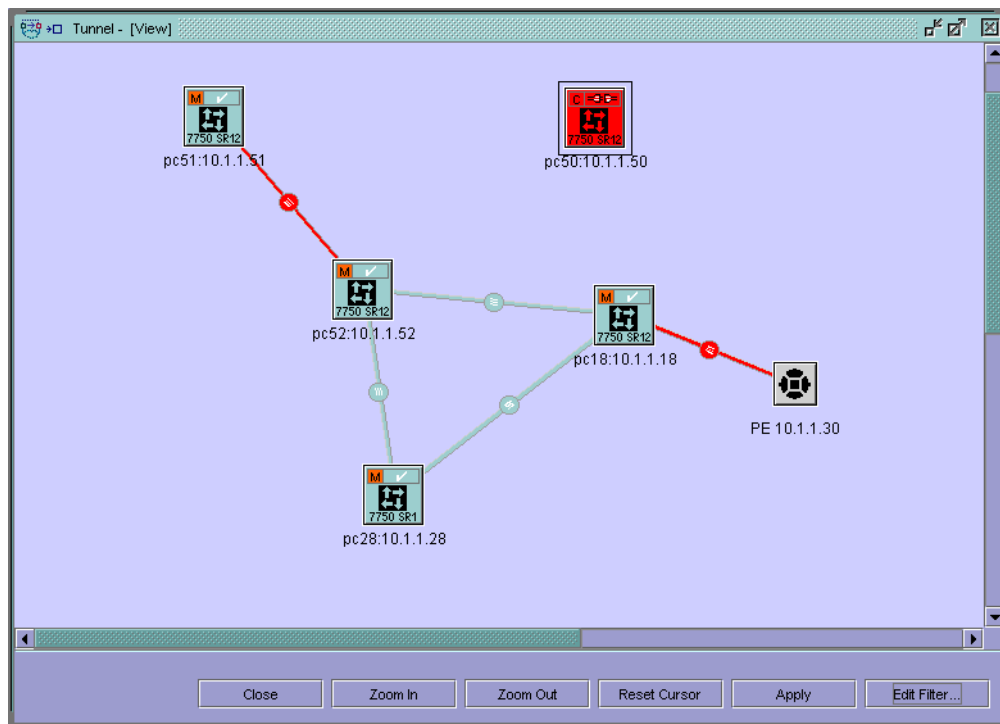
In this context, the service map that appears displays all devices for the service. Right-click on the device to open contextual menus and submenus for the device. The symbol and color in the top left corner of the managed device icon represent the most severe alarm on the device. The symbol and color in the top right corner represent the status of any of the device.

Link groups between devices represent service circuits. Link groups between device icons and ports represent the binding of an access port or interface to a service. Right-click on the link group icon to open contextual menus and submenus. Right-click anywhere on the service map to open contextual menus and submenus for all the sites for the service.

Service path topology maps

A service tunnel map view is available on the 5620 SAM by choosing Topology→Service Path Topology from the 5620 SAM main menu. Configure the network filter parameters in the form that appears and click on the OK button. The Service Path topology map appears, as displayed in Figure 27-5.

Figure 27-5 Service path topology map



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

27.2 Map management workflow

- 1 Determine the map view you want to use. You can:
 - view maps that show services
 - view maps that show topology
- 2 View the relationship between objects drawn on the map:
 - services show which network elements are used by the services
 - topology maps show the appropriate relationship between network elements in the routing domain.

27.3 Map menus

Table 27-1 lists the map menus and the tasks they perform.

Table 27-1 5620 SAM map menus

Menu option	Function
Topology→Service Path Topology	Type of map
Topology→LSP Topology	Type of map
Topology→MPLS Path Manager	Type of map
Topology→LSP Manager	To create LSPs, rather than view them. See chapter 18 for more information.
Topology→Service Tunnel Manager	To create service tunnels, rather than view them. See chapter 19 for more information.

27.4 Map management procedures list

Table 27-2 lists the procedures to perform map management tasks.

Table 27-2 5620 SAM map procedures list

Procedure	Purpose
To open a map	Open a map from the main menu.
To view and understand map elements	Interpret the map elements

(1 of 2)

Procedure	Purpose
To open the LSP path map from the MPLS Path Manager	To view a specific LSP path in context of its source, and transient and destination hops
To open the LSP path map from the LSP Path Manager	To view a specific LSP path in context of its source, and transient and destination hops
To list or view object information from a map	To find and open the appropriate contextual menu from map objects.
To zoom in and zoom out of a map	To manipulate the size of objects displayed on the map.

(2 of 2)

27.5 Map management procedures

Use the following procedures to perform map management tasks.

Procedure 27-1 To open a map

- 1 Choose Topology → *Option* from the 5620 SAM main menu, where *option* is a menu option as described in step 2.

The menu options appear.

- 2 Choose a type of map to view from the menu options.
 - a Service Path Topology to view service paths.
 - b LSP Topology to view LSPs
 - c MPLS Path Manager to view MPLS paths.
 - d LSP Manager to view LSP paths.
 - e Service Tunnel Manager to view service tunnels.

The appropriate filter form appears.

- 3 Create a filter to narrow the range of objects that will be displayed on the map. The options that appear depend on the choice made in step 2.
- 4 Click on the OK or Search button.

The map is refreshed or appears showing the filtered network objects.

Procedure 27-2 To view and understand map elements

- 1 Open a map as indicated in Procedure 27-1.

- 2 View the map information. Figure 27-1 shows the map main elements.
 - The icon in the top left corner of device icons represent the most serious alarm raised against the device.
 - The icon in the top right corner of device icons represents the connectivity to the device.
 - The color in the body of the device icon represents connectivity.
 - red means down or unreachable
 - yellow means reconciling or discovering
 - green means normal
-

Procedure 27-3 To open the LSP path map from the MPLS Path Manager

- 1 Choose Topology→MPLS Path Manager from the 5620 SAM main menu.

The Search form appears.
 - 2 Create an appropriate filter and click on the Search button.

The list of filtered MPLS paths appear.
 - 3 Choose an MPLS path from the list.
 - 4 Click on the Edit button.

The MPLS path configuration form for the MPLS path appears.
 - 5 Click on the Provisioned Path tab button.

The hops of the MPLS path appear.
 - 6 Choose a hop from the list.
 - 7 Click on the Topology View button.

The map appears showing the hops between the devices.
-

Procedure 27-4 To open the LSP path map from the LSP Path Manager

- 1 Choose Topology→LSP Manager from the 5620 SAM main menu.

The Search form appears.
- 2 Create an appropriate filter and click on the Search button.

The list of filtered LSPs appears.
- 3 Choose an LSP and click on the Edit button.

The LSP configuration form appears.

- 4 Click on the LSP Paths tab button.

The list of LSP paths appears.

- 5 Choose a path from the list and click on the Edit button.

The LSP path configuration form appears.

- 6 Click on the Provisioned Path tab.

The hops of the LSP path appear.

- 7 Choose a hop from the list.

- 8 Click on the Topology button.

The map appears showing the hops between the devices.

Procedure 27-5 To list or view object information from a map

- 1 Open a map as indicated in Procedure 27-1.
 - 2 Right-click on an appropriate object.
 - a A device icon.
 - b A circle or arrow in the centre of a link or path group.
 - c A port of custom node indicating the end-point of a link, path, tunnel, or service.

The appropriate contextual menu appears.
 - 3 Navigate through the available contextual menu options to find
 - 4 Navigate through the available contextual menu options. You can do the following, depending on the object selected in step 2.
 - View a list of network objects, for example, the service tunnels of LSPs running in the group chosen. You can then choose one and view or edit its configuration.
 - Create new connections between the devices, as appropriate.
 - View the properties of the object such as a 7450 ESS. You can then view or edit the device configuration.
-

Procedure 27-6 To zoom in and zoom out of a map

- 1 Open a map as indicated in Procedure 27-1.
- 2 Click on the Zoom in or Zoom out button.
- 3 Move your cursor into the map pane.

The icon changes to a magnifying glass containing a + or - sign.

- 4** Click on the area of the map you want to expand or contract.

The map expands or contracts. Continue clicking the mouse until the desired zoom level is reached.

Use the opposite button and an equal number of clicks to return the map to its default setting.

- 5** Click on the Reset Cursor button to return to the pointer icon.
-

Fault management

28 — Fault management using alarms

29 — Troubleshooting and fault management using OAM

28 — *Fault management using alarms*

- 28.1 Fault management using alarms overview 28-2**
- 28.2 Workflow to manage network faults using alarms 28-4**
- 28.3 Fault management alarms menus 28-5**
- 28.4 Fault management using alarms procedures list 28-5**
- 28.5 Fault management using alarms procedures 28-6**
- 28.6 Alarm descriptions 28-20**

28.1 Fault management using alarms overview

The 5620 SAM converts SNMP traps from network devices to events and alarms. These are then correlated against the managed equipment and configured services and policies. Alarms are applied against the appropriate equipment and services.

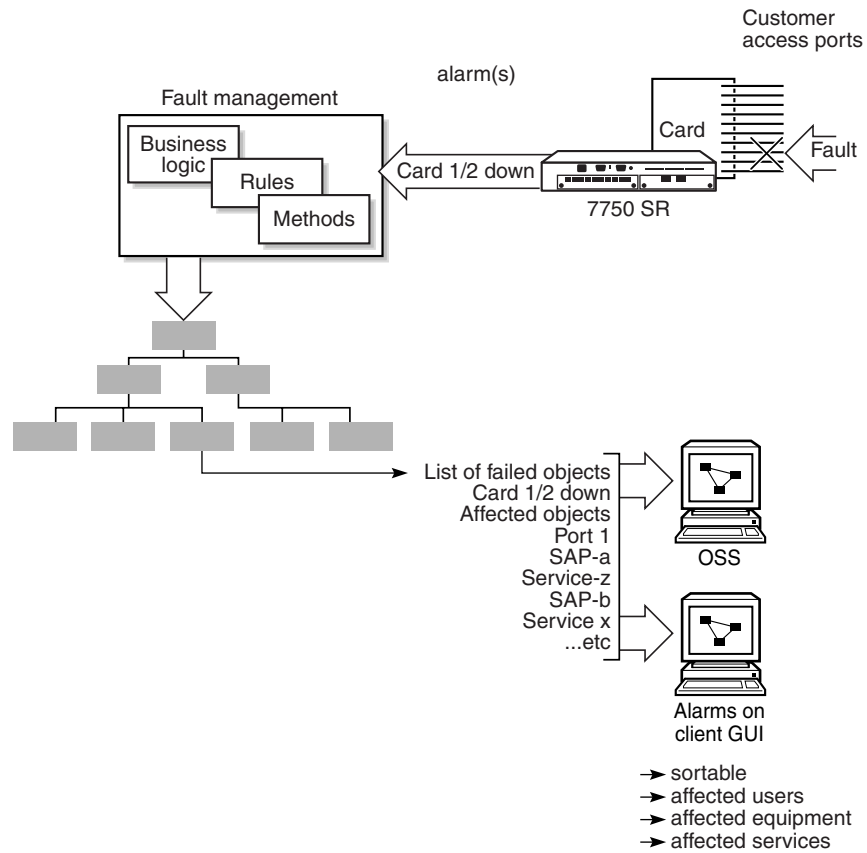
The fault management system provides:

- conversion of SNMP traps to many X.733-standard alarm fields
- impact analysis and correlation of alarms to equipment and service-affecting faults
- updated operational status of equipment, services, and interfaces in near-real-time from the network device resources
- alarm policy control by network administrators so the administrators can determine how to handle individual incoming alarms and how alarm logs are created and stored
- point-and-click alarm management from both the dynamic alarm list and from equipment and services configured on the 5620 SAM GUI
- operator notes and acknowledgement to track the work undertaken to fix the problem that caused the alarm
- correlated data in a historical alarm database to provide trend analysis and records

Correlated alarms mean that one alarm may cause fault conditions for many other objects. When alarms are correlated, the alarms may appear in multiple places. For example, if an alarm is raised because a port goes down, any services using that port would receive indication of the alarm, viewable from the service configuration form, or from the subscriber information form that lists the affected service. This means that all object information forms contain a faults tab, which lists alarms affecting the object. All alarms appear on the dynamic alarm list.

Figure 28-1 shows how alarms are handled by the fault management system.

Figure 28-1 Alarm handling

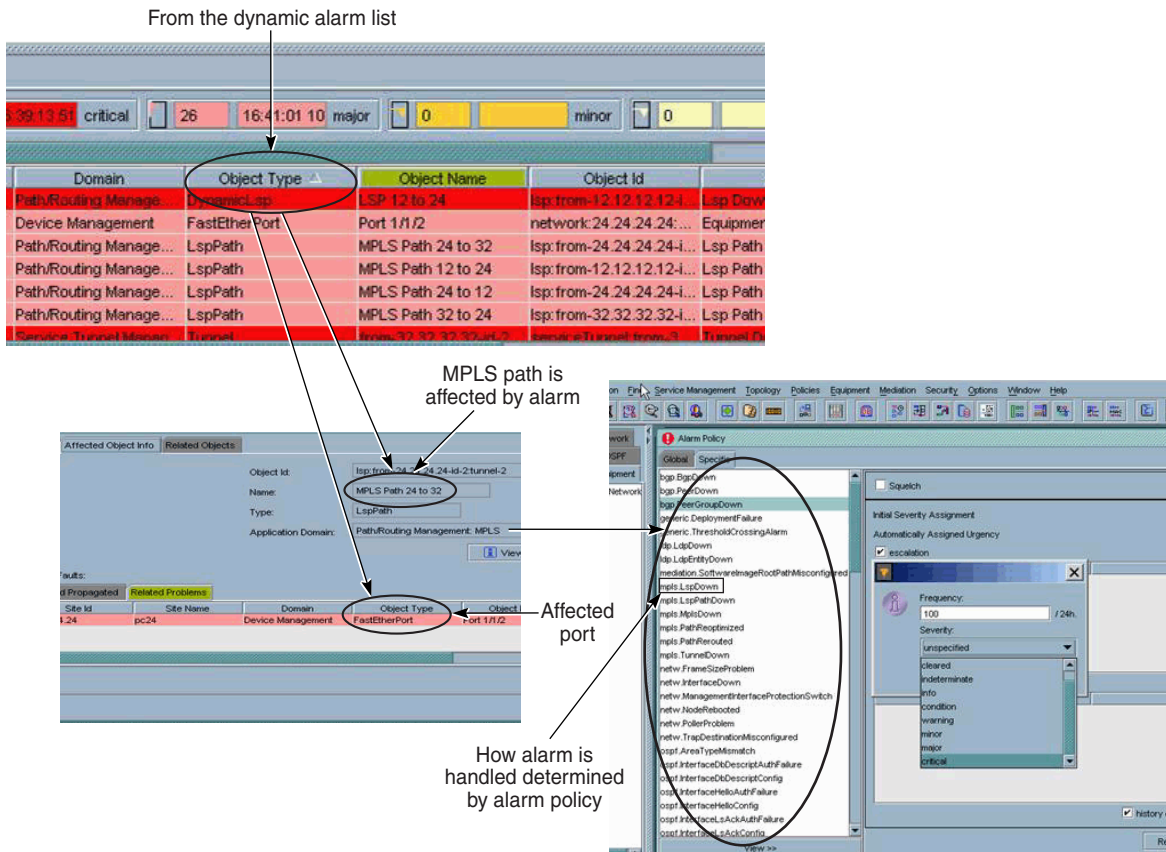


17167

Figure 28-2 shows the following alarm relationships on the GUI between:

- incoming alarms and the dynamic alarm list
- display of object alarm
- impact of the alarm policy parameter settings on the alarm

Figure 28-2 Alarm relationships on the GUI



Alarm severity is indicated on the GUI by color. The color code used is consistent anywhere on the GUI.

- red for critical alarms
- pink for major alarms
- yellow for minor alarms
- tan for warning alarms
- grey-blue for acknowledged alarms

28.2 Workflow to manage network faults using alarms

- 1 Set up the 7750 SRs to send SNMP traps of faults and events to the 5620 SAM. See the *7750 SR OS System Guide* for more information.
- 2 Set alarm policies on the 5620 SAM using the Policies→Alarm Policies:
 - i Set global policies for incoming alarms.
 - ii Set specific policies for each alarm type.
 - iii Set alarm history policies for the storage of alarms.

- 3 Set alarm options using the Options menu. Choose to enable or disable the alarm bell when an incoming alarm is registered.
- 4 Monitor alarms:
 - i For SLAs by monitoring SAP and subscriber service alarms.
 - 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.
 - iii For the network from the dynamic alarm list.
 - iv For incoming SNMP traps from 7750 SRs by viewing logs.

See section 28.6 for a list of alarms converted from SNMP traps.
- 5 Reset alarm policy based on changing network and new alarm support requirements.
- 6 Review historical alarms in the database for trends and store the alarms for record-keeping.

28.3 Fault management alarms menus

Table 28-1 lists the fault management menus and their functions.

Table 28-1 5620 SAM fault management menus

Menu option	Function
Policies→Alarm Policies	Set alarm policies for all incoming alarms, alarm types, and historical alarm storage.
Options→Disable Audible Alarms	Enable or disable the incoming alarm bell.
Find→Browse Alarm History	Review historical alarms for trends.

28.4 Fault management using alarms procedures list

Table 28-2 lists the procedures necessary to execute fault management tasks.

Table 28-2 5620 SAM fault management procedures list

Procedure	Purpose
To set global alarm policies	Specify how incoming alarms are handled.
To set alarm history behavior	Determine the parameters for alarms are stored in the database.
To set specific alarm policies	Specify the behavior of one or more incoming alarms.

(1 of 2)

Procedure	Purpose
To view alarms raised against equipment, logical components, and services	View specific faults on the equipment.
To view alarm information	View all alarm information fields.
To view all network alarms using the dynamic alarm list	View all incoming network alarms.
To view network alarm statistics	View statistics related to all incoming network alarms.
To review historical alarms	Review records and trend analysis.

(2 of 2)

28.5 Fault management using alarms procedures

Use the following procedures to perform fault management tasks.

Procedure 28-1 To set global alarm policies

Global alarm policies affect all network alarms, and can be set by users with system administration privileges.

- 1 Choose Policies→Alarm Policies from the 5620 SAM main menu.
The Alarm Policy form appears
- 2 Click on the Global tab button.
- 3 Click on the Alarm Behavior tab button.
- 4 Set the severity policies by clicking on the Severity tab button:
 - i Select the Severity Alterable check box 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.

Figure 28-3 shows the Alarm Policy configuration form with the Severity tab selected.

Figure 28-3 Alarm Policy configuration form - Severity

Severity cannot be altered unless the check box is enabled.

- Select the manual severity alterations check box to allow operators to manually change severity for alarms. You can then choose one or more sub-options:
 - Choose the severity promotion option to allow an operator to increase the severity of an alarm.
 - Choose the severity demotion option to allow an operator to decrease the severity of an alarm.
 - Choose the clearing (if not one-shot alarm) option to allow the operator to clear an alarm.
 - Select the automatic severity alterations check box to enable automatic severity changes for alarms based on specific alarm policies. You can then choose one or more sub-options:
 - Choose the implicit severity promotion option to promote the severity of the alarm based on the specific alarm policy.
 - Choose the implicit severity demotion option to demote the severity of the alarm based on the specific alarm policy.
 - Choose the Escalation (defined by specific policy) option to escalate the severity of an alarm based on the specific alarm policy.
 - Choose the de-escalation (defined by specific policy) option to de-escalate the severity of an alarm based on the specific alarm policy.
- ii Choose the appropriate severity policies from the list of options. Set new severities based on your network requirements.
- 5 Set the deletion policies by clicking on the Deletion tab button:
- i Select the Alarm deletion check box to allow the creation 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.
 - Under the manual heading, choose one manual deletion policy:
 - Choose the disable option to never allow the deletion of alarms.
 - Choose the when cleared option to allow the deletion of the alarm after it is cleared.
 - Choose the when acknowledged option to allow the deletion of the alarm after it has been acknowledged.
 - Choose the when cleared and acknowledged option to allow the deletion of the alarm after both conditions are met.
 - Choose the when cleared or acknowledged option to allow the deletion of the alarm after one of the conditions is met.
 - Choose the always option to allow the deletion of the alarm at any time.
 - Under the auto heading, choose one automatic deletion policy:
 - Choose the disabled option to never allow the automatic deletion of alarms.
 - Choose the when cleared option to allow the automatic deletion of alarms after they are cleared.
 - Choose the when acknowledged option to allow the automatic deletion of alarms after the alarms have been acknowledged
 - Choose the when cleared and acknowledged option to allow the automatic deletion of alarms after both conditions are met
 - Choose the when cleared or acknowledged option to allow the automatic deletion of alarms after one of the conditions is met
- 6 Click on the Apply button to save the changes.
 - 7 Click on the OK button to close the form.
-

Procedure 28-2 To set alarm history behavior

The 5620 SAM stores new and old alarms for record-keeping and trend analysis. You can specify how alarms are stored in the database.

- 1 Choose Policies→Alarm Policies from the 5620 SAM main menu.

The Alarm Policy form appears.
- 2 Click on the Global tab button.
- 3 Click on the Alarm History DB Behavior tab button.
- 4 Set the alarm history behavior:
 - a Specify the Max Log Size (records) parameter to set the maximum size of the alarm history log. You can store more than 1,000,000 historic alarms in the alarm history log.

- b** Specify what action the 5620 SAM takes when the alarm history log exceeds the maximum log size by setting the Log Full Action and Clear Window (records) parameters. By default, the Clear Window (records) parameter is set to delete 500 alarm history log records when the log is full using the Log Full Action parameter Round Robin option.
- c** Set the Administrative State parameter to Up to enable alarm history logging.
- d** Select the Log on Change check box to specify whether to log an alarm when one of its properties changes, for example, to log an alarm when the alarm is acknowledged.
- e** Select the Log on Deletion check box to specify whether to log an alarm when it is deleted.



Note — Alcatel recommends using the Log on Deletion option, to ensure historical log records of all deleted alarms exists.

- f** Set filters to the DB policy to determine the criteria for an alarm to be logged:
 - i** Click on the Edit Filter button.
The Alarm History Filter form appears.
 - ii** Choose the filter type by selecting one or more filters from the Unused Properties list. The Unused Properties list shows all the alarm record fields.

To ensure a complete history log, filter alarms based on a criteria that all alarms will share. For example, if your policy is to ensure all alarms have severity of Cleared, choose Severity from the Unused Properties list.
 - iii** Click on the right-facing arrow to move the selected filters to the Filtered Properties list.
 - iv** Configure the properties of the alarm information field to determine how filtering is done.

For example, set Severity to equal a state of cleared. This ensures that all alarms set to Cleared are sent to the alarm history log.
 - v** Click on the OK button.



Caution — Purged alarms are not logged, and cannot be retrieved.

- g** Purge alarms with the Purge All or Purge Range button. The Purge Range button can be used when a filter policy is applied.

Procedure 28-3 To set specific alarm policies

Specific alarm policies allow you to modify the behavior of one or more specific types of alarms, if you want that alarm to behave differently than the default.

- 1 Choose Policies→Alarm Policies from the 5620 SAM main menu.

The Alarm Policy form appears.

- 2 Click on the Specific tab button.

A list of alarm types appears.

- 3 Choose an alarm type from the left hand column.

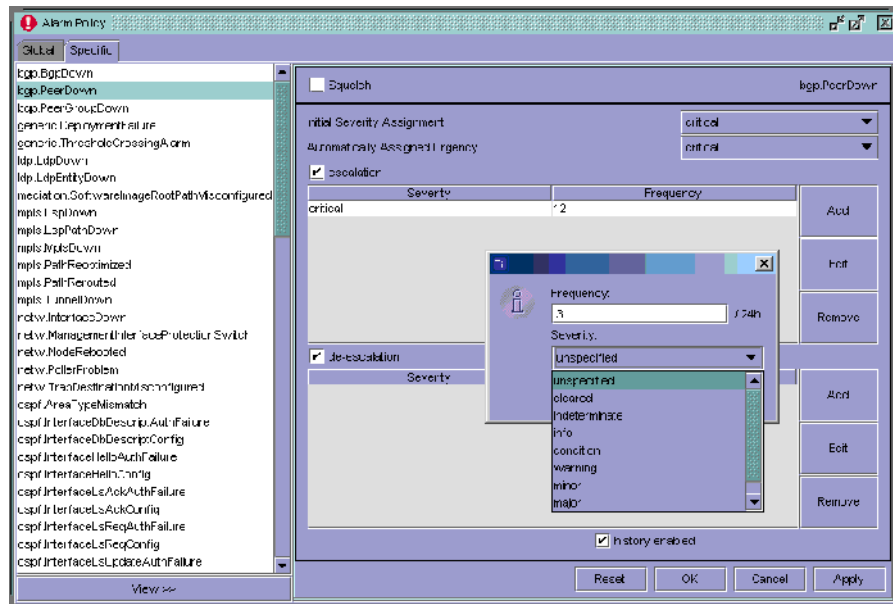
The alarm types are listed by their SNMP trap name. A list of alarms using the GUI names is available in Table 28-5.

- 4 Click on the View>> button.

The name of the alarm appears in the top right panel.

Figure 28-4 shows a sample configuration form.

Figure 28-4 Alarm policy configuration form



- 5 Set the policies for the selected alarm:
 - a Select the Squelch check box to ignore every instance of the alarm.
 - b Use the drop-down menus to set the Initial Severity Assignment and the Automatically Assigned Urgency parameters of the alarm.
 - c 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 or de-escalation check box.
- ii Click on the Add button.
- iii Set the Frequency in a 24-h period. This is the threshold of how often the alarm must arrive before the severity is escalated or de-escalated.
- iv Use the Severity parameter to specify the new severity applied against the alarm if the escalation or de-escalation threshold is reached.
- v Use the history enabled parameter to specify whether an entry should occur in the log each time a policy is applied to change the severity level of an alarm.
- vi Click on the Apply button.

The new escalation or de-escalation policy is applied to the alarm.

Procedure 28-4 To view alarms raised against equipment, logical components, and services

Alarms raised against network objects allow you to view faults on each device in the network down to the service, path, or port level. The 5620 SAM correlates 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 Self and Propagated and Related Problems tabs. These tabs show alarms against specific objects, such as ports, and related problems, such as services that use the ports.

- 1 Choose:
 - a Equipment→Equipment Manager from the 5620 SAM main menu to view equipment alarms. Go to step 2.
 - b Another menu that displays a path, logical component, service, or subscriber form.

The form appears. Go to step 4.

- 2 Choose a network element from the drop-down list.
- 3 Click on one of the following types of equipment that you want to view. You can choose from:
 - shelf
 - card slot
 - cards
 - ports
 - channels
 - daughter card slots
 - daughter cards
 - interfaces
- 4 Click on the Faults tab button.

A list of alarms appears under the appropriate tabs.

- 5 Review the alarm information. See Table 28-3 for the type of information available in an alarm. The list of possible alarms is displayed in the right-hand panel of the Specific tab of the Alarm Policy form.
 - a Scroll across each line to view the information contained in the alarm.
 - b Double-click on the line to open the alarm info form for the specific object.
 - c Click on the Related Object tab, from the Affected Object Info tab, to view alarms that generally affect the device or service.
 - d Click on the Affected Object Info tab button to navigate to the affected object.
 - 6 Handle alarms according to your fault management policies. See section 28.6 for a list of alarms converted from SNMP traps.
-

Procedure 28-5 To view alarm information

Alarm information is available from:

- the dynamic alarm list
- the equipment fault tab alarm list
- policy, service, and other fault tabs
- the alarm information form when you double-click on a row in an alarm list

- 1 Click on the appropriate fault tab.

Fault tabs include tabs listing alarms against the specific object, and alarms against related objects that affect the specific object.

- 2 Open an alarm from a list by selecting an alarm from the list and clicking on the Edit button. Alternately, you can double-click on the alarm in the list.



Note — GUI performance can suffer when sorting more than 15,000 outstanding or logged alarms. Use filters to ensure that a reasonable number of alarms are listed.

Figure 28-5 shows an Alarm Info form.

Figure 28-5 Alarm Info form - Info

Alarm Info: faultManager:network@10.1.1.18@pppSite@ppp-1/589332547[alar...

Alarm Affected Object Info Related Objects

Info Severity Statistics Acknowledgement

Application Domain: ppp

Site Id: 10.1.1.18

Site Name: pc18

Affected Object Type: Interface

Affected Object Name: ppp-1/589332547

Affected Object Id: network:10.1.1.18;pppSite:ppp-1/589332547

Alarm Name: Frame Size Problem

Alarm Type: Configuration Alarm

Alarm Severity: critical

Alarm Cause: Frame Size Problem

Acknowledged:

Acknowledged By: N/A

Time Detected: 03/24/2004 16:30:17 574 EST

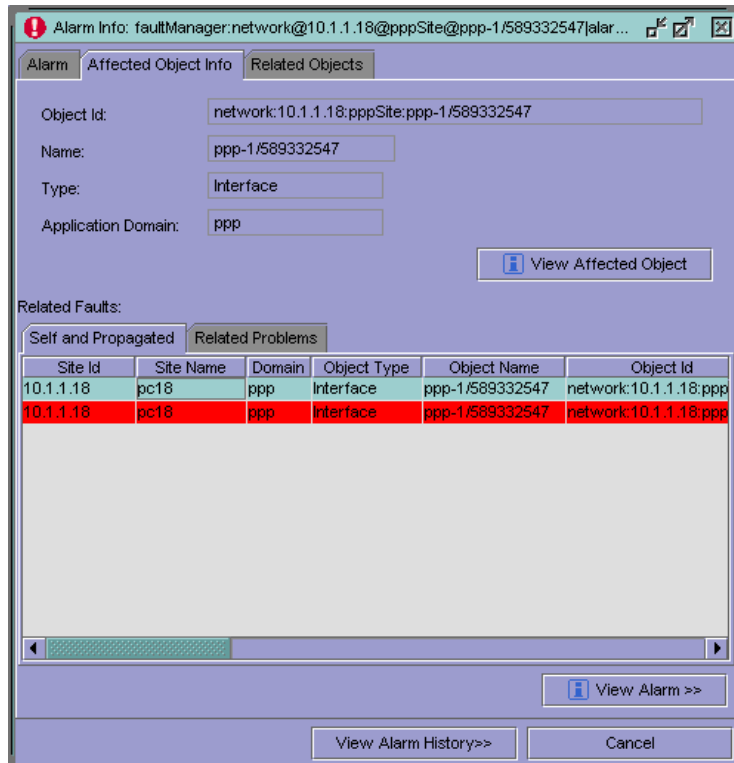
Additional Text: N/A

Delete Clear Acknowledge View Policy

View Alarm History>> Cancel

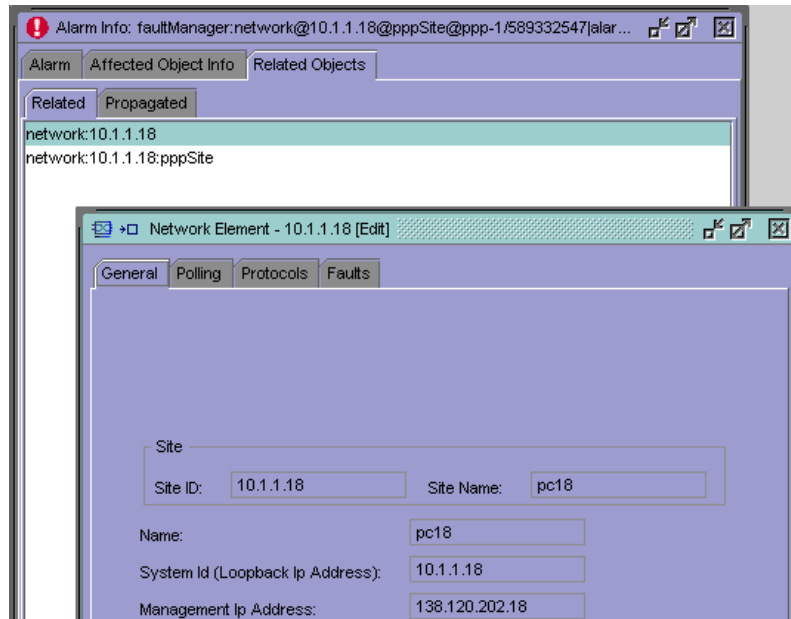
- 3 Review the alarm information.
 - a Click on the Affected Object Info tab button to navigate to the affected object. Figure 28-6 shows a sample affected object tab for an alarm.

Figure 28-6 Alarm Info - Affected Object Info



- b Click on the Related Objects tab to view other network objects that are affected by this alarm. Figure 28-7 shows a sample related object form and the configuration form for the related object.

Figure 28-7 Alarm Info form - Related Objects



- c View the alarm information in each tab and respond according to your alarm-handling policies.

Table 28-3 lists the types of alarm information available to users from the Alarm Info form. Section 28.6 lists the alarms converted from SNMP traps.

Table 28-3 Alarm information from the Alarm Info form

Alarm field	Information
Alarm row from list or Info tab on Alarm Info form	
Application domain	The general area of the 5620 SAM software that is affected by the alarm. This is of particular interest and use to those monitoring alarms using the XML OSS interface. See the <i>5620 SAM-O OSS Interface Developer Guide</i> for more information.
Site ID	IP address of the router issuing the alarm
Site Name	Name of the router
Object Type	Type of object
Affected Object Type	
Object Name	Name of the object
Affected Object Name	
Object Id	Unique string identifying the object down to the lowest level, for example, network ID #, chassis #, slot #, daughterCardSlot #
Affected Object Id	
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	
Cause	Vendor-specific and X.733 standards for the probable cause of the alarm
Alarm Cause	
Severity	Vendor-specific, TMN, and X.733 standards for severity of the alarm
Alarm Severity	
Ack	Whether the alarm has been acknowledged by an operator (true) or not (false)
Acknowledged	
Acknowledged By	Name of operator that acknowledged the alarm
Urgency	Urgency setting of the alarm
Effect on Service	Whether an equipment alarm has affected a customer service (true or check mark) or not (false or no check mark)
Service Affecting	
Severity tab on Alarm Info form	
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.

(1 of 2)

Alarm field	Information
Statistics tab on Alarm Info form	
Frequency Number of Occurrences Number of Occurrences Since Clear Number of Occurrences Since Ack.	How often the alarm has been raised, based on the specified scenarios. You can modify the alarm frequency by clicking on the View Policy button and modifying the individual alarm settings. You can delete, clear to the historical database, acknowledge, or view the history of the alarm.
Acknowledgement tab on Alarm Info form, Acknowledgement Info tab selected	
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. You can delete, clear to the historical database, acknowledge, or view the history of the alarm.
Acknowledgement tab on Alarm Info form, Notes tab selected	
View button Edit button New 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.
Affected Object Info tab on Alarm Info form	
Object Id	The unique instance of the object in the network.
Name	The name of the object that generated the alarm.
Type	The type of object that generated the alarm.
Application Domain	The general area of the 5620 SAM software that is affected by the alarm. This is of particular interest and use to those monitoring alarms using the XML OSS interface. See the <i>5620 SAM-O OSS Interface Developer Guide</i> for more information.
Related faults tabs	Click on the tabs to view alarms related to the currently viewed alarm.
View Affected Object button	Click on the View Affected Object button to open the appropriate form or list for the object that has the alarm raised against it.
Related Objects tab on the Alarm Info form	
Related tab	A hierarchical tree showing the network object Id of the object that raised the alarm, from the IP address of the device to the affected chassis, slot, card, MDA, and port, if applicable. Related objects are objects that are affected by an alarm because of a relationship between objects, for example, when a port is down, then service access points that terminate on the port are down.
Propagated tab	The propagated tab displays: <ul style="list-style-type: none"> alarms raised due to explicit dependencies between network objects network objects affected by an alarm because of object containment, for example, when a card is down all ports on the card are down
View Object button	Click on the View Object button to open the appropriate form or list for the related object that has been affected by the generated alarm.

(2 of 2)

- Handle the alarm according to your company's alarm handling policy:

- a Click on the Delete button to delete the alarm, if you have permissions to delete alarms.



Caution — You cannot recover a deleted alarm.

- b Click on the Clear button to clear the alarm. The alarm is cleared from the list, and is added to the alarm log if it meets the filtering criteria.
- c Click on the Acknowledge button to acknowledge the alarm.
 - i From the Note tab button, modify the urgency and assigned severity of the alarm using the Urgency, Assigned Severity, and Acknowledgement parameters, if applicable, and if you have permissions to modify the alarm.
 - ii Add a note to the alarm from the Notes tab button and click on the Apply button.
 - iii Click on the Ok button to acknowledge the alarm.

The alarm is acknowledged. 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
- d Click on the View Policy button. The Alarm Policy form appears with the alarm type selected on the Specific tab. You can view the policy configured for the alarm type, as described in Procedure 28-3.
 - e Click on the View Alarm History>> button to view the alarm log for this type of alarm. An Alarm History Filter window appears with the Alarm Name filter equal to the type of alarm you are viewing.
 - i Click on the OK button to specify the filter. By default, the filter is set to look for the same alarm type you are currently viewing.

A list of alarm history records appears.
 - ii Choose the record from the alarm history log, as described in Procedure 28-8.

Procedure 28-6 To view all network alarms using the dynamic alarm list

The dynamic alarm list allows you to monitor incoming faults from the devices and software. This feature is most useful when monitoring the network. Figure 28-8 shows the dynamic alarm list.

Figure 28-8 Dynamic alarm list

Site ID	Site Name	Domain	Object Type	Object Name	Object ID	Alarm	Time Deleted
10.1.1.35	pc35	netw	NetworkElement	pc35	network:10.1.1.35	Poller Problem	10/29/2003 13:12:52.5... Commun
10.1.1.35	pc35	netw	NetworkElement	pc35	network:10.1.1.35	Trap Destination Miss	10/29/2003 13:12:52.4... Configu

- 1 Click on the Alarm Table tab button from the bottom of the 5620 SAM client GUI. The dynamic list of incoming network alarms appears.



Note — GUI performance can suffer when sorting more than 15,000 outstanding or logged alarms. Use filters to ensure that a reasonable number of alarms are listed.

The color bar under the Alarm Table tab indicates the number of alarms of each type in the dynamic list, color-coded by severity.

- 2 Right-click on an alarm entry row. The contextual alarm menu appears.
- 3 Choose:
 - a Show Alarm(s) to view the alarm info form. Table 28-3 lists the alarm information displayed.
 - b Show Affected Object to display the configuration form for the object against which the alarm is raised.
 - c Acknowledge Alarm(s) to open the acknowledgement form.
 - d Assign Severity to change the severity policy of the alarm.
 - e Delete Alarm(s) to delete the alarm.



Caution — You cannot recover a deleted alarm.

- f Clear Alarm(s) to clear the alarm.
- g CLI→*option* to start a SSH or Telnet CLI session with the managed equipment that generated the alarm.
- h 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 Cancel button to return to the dynamic alarm list.

- 4 Handle the alarm(s) according to your fault management policies. Alarm handling is described in Procedure 28-5.

After alarms are cleared or deleted, the alarms are stored in the alarm log if they meet the filter criteria.

Procedure 28-7 To view network alarm statistics

- 1 Click on the Alarm Statistics tab button in the dynamic alarm list.

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 acknowledgement and service-affecting status, and then by the number of critical, major, minor, warning, condition, info, indeterminate, and cleared alarms.

Procedure 28-8 To review historical alarms

Alarms that meet filtering criteria are logged in an alarm log.

- 1 Choose Find→Browse Alarm History from the 5620 SAM main menu.

The Alarm History Filter form appears.

- 2 If required, choose a filter to narrow the range of historical alarms displayed.
- 3 Click on the OK button.
- 4 The historical alarms appear based on the filtering criteria.



Note — When sorting alarms, sorting more than 15,000 outstanding or logged alarms may slow GUI performance. Use filters to ensure that a reasonable number of alarms are listed.

Table 28-3 lists the information displayed for each alarm. Table 28-4 lists the additional historical alarm information available from the alarm history form for logged alarms.

Table 28-4 Additional information for logged alarms

Alarm field	Information
Time Logged	Time stamp of when alarm was moved to the historical alarm database
Alarm Status	Reason the alarm was logged to the historical alarm database
First Time Detected	Time of the first recorded instance of the alarm
Last Time Detected	Time of the last recorded instance of the alarm
Number Of Occurrences	How often the alarm was sent

- 5 Manage the logged alarms:
 - a Click on the Edit Policy button to view or change the parameters of how alarms are logged. See Procedure 28-2 for more information.
 - b Click on the Purge Filtered button to purge alarms that meet the purging criteria.
 - c Click on the Edit Filter button to narrow the list of logged historical alarms.
 - d Click on the Refresh button to update the list of logged alarm displayed in the form.
- 6 Click on the Close button to close the form.
- 7 Click on the Cancel button to close the Alarm Filter History form.

28.6 Alarm descriptions

Table 28-5 describes the alarms.

Table 28-5 Alarm descriptions

Alarm name, type, and default probable cause	Severity, object type, and domain
Name: Bgp Down Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Site Domain: bgp
Name: Peer Connection Down Type: Protocol Alarm Probable cause: connectionDown (2)	Severity: critical Object type: Peer Domain: bgp
Name: Peer Down Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Peer Domain: bgp

(1 of 12)

Alarm name, type, and default probable cause	Severity, object type, and domain
Name: Peer Group Down Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: PeerGroup Domain: bgp
Name: Prefix Limit Exceeded Type: Protocol Alarm Probable cause: Prefix Limit Exceeded	Severity: major Object type: Peer Domain: bgp
Name: Prefix Limit Nearing Type: Protocol Alarm Probable cause: Prefix Limit Nearing	Severity: warning Object type: Peer Domain: bgp
Name: Equipment Down Type: Equipment Alarm Probable cause: Inoperable Equipment	Severity: major Object type: Equipment Domain: equipment
Name: Equipment In Test Type: Equipment Alarm Probable cause: Equipment In Test	Severity: warning Object type: Equipment Domain: equipment
Name: Equipment Mismatch Type: Equipment Alarm Probable cause: Equipment Type Mismatch	Severity: major Object type: Equipment Domain: equipment
Name: Equipment Removed Type: Equipment Alarm Probable cause: Replaceable Equipment Removed	Severity: major Object type: Equipment Domain: equipment
Name: Link Down Type: Communications Alarm Probable cause: Port Link Problem	Severity: major Object type: Equipment Domain: equipment
Name: Temperature Threshold Crossed Type: Environmental Alarm Probable cause: Equipment Overheated	Severity: major Object type: Environment Domain: equipment
Name: Deployment Failure Type: Deployment Failure Probable cause: Failed To Modify Network Resource	Severity: minor Object type: Generic Object Domain: generic
Reserved for testing	—
Reserved for testing	—
Reserved for testing	—
Reserved for testing	—
Name: Threshold Crossing Alarm Type: ThresholdCrossed Probable cause: Threshold Crossed	Severity: warning Object type: Generic Object Domain: generic
Name: Isis Down Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Site Domain: isis
Name: Lag Down Type: Equipment Alarm Probable cause: Lag Down	Severity: critical Object type: Interface Domain: lag

(2 of 12)

Alarm name, type, and default probable cause	Severity, object type, and domain
Name: Ldp Down Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Site Domain: ldp
Name: Ldp Interface Down Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Interface Domain: ldp
Name: Ldp Targeted Peer Down Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Targeted Peer Domain: ldp
Name: Software Image Root Path Misconfigured Type: Configuration Alarm Probable cause: File Path Problem	Severity: warning Object type: Software Upgrade Policy Domain: mediation
Name: Lsp Down Type: Path Alarm Probable cause: Lsp Down	Severity: critical Object type: Lsp Domain: mpls
Name: Lsp Path Down Type: Path Alarm Probable cause: Lsp Path Down	Severity: major Object type: Lsp Path Domain: mpls
Name: Mpls Down Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Site Domain: mpls
Name: Path Reoptimized Type: Path Alarm Probable cause: Path Reoptimized	Severity: warning Object type: Tunnel Domain: mpls
Name: Path Rerouted Type: Path Alarm Probable cause: Path Rerouted	Severity: warning Object type: Tunnel Domain: mpls
Name: Tunnel Down Type: Path Alarm Probable cause: Tunnel Down	Severity: warning Object type: Tunnel Domain: mpls
Name: Boot Parameters Misconfigured Type: Configuration Alarm Probable cause: Persistent Index Failure	Severity: critical Object type: Network Element Domain: netw
Name: Frame Size Problem Type: Configuration Alarm Probable cause: Frame Size Problem	Severity: critical Object type: Statefull Connectable Interface Domain: netw
Name: Interface Down Type: Interface Alarm Probable cause: Interface Down	Severity: critical Object type: Statefull Connectable Interface Domain: netw
Name: Management Interface Protection Switch Type: Communications Alarm Probable cause: Switch To Secondary	Severity: warning Object type: Network Element Domain: netw

(3 of 12)

Alarm name, type, and default probable cause	Severity, object type, and domain
Name: Node Rebooted Type: Equipment Alarm Probable cause: Node Reboot	Severity: warning Object type: Network Element Domain: netw
Name: Poller Problem Type: Communications Alarm Probable cause: Resync Failed	Severity: warning Object type: Network Element Domain: netw
Name: Trap Destination Misconfigured Type: Configuration Alarm Probable cause: Trap Destination Misconfigured	Severity: major Object type: Network Element Domain: netw
Name: Area Type Mismatch Type: Configuration Alarm Probable cause: Area Type Misconfigured	Severity: warning Object type: Area Domain: ospf
Name: Interface Db Descript Auth Failure Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Interface Domain: ospf
Name: Interface Db Descript Config Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Interface Domain: ospf
Name: Interface Hello Auth Failure Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Interface Domain: ospf
Name: Interface Hello Config Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Interface Domain: ospf
Name: Interface Ls Ack Auth Failure Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Interface Domain: ospf
Name: Interface Ls Ack Config Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Interface Domain: ospf
Name: Interface Ls Req Auth Failure Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Interface Domain: ospf
Name: Interface Ls Req Config Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Interface Domain: ospf
Name: Interface Ls Update Auth Failure Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Interface Domain: ospf
Name: Interface Ls Update Config Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Interface Domain: ospf

(4 of 12)

Alarm name, type, and default probable cause	Severity, object type, and domain
Name: Interface Null Packet Auth Failure Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Interface Domain: ospf
Name: Interface Null Packet Config Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Interface Domain: ospf
Name: Interface Rx Bad Packet Type: Communications Alarm Probable cause: Hello	Severity: warning Object type: Interface Domain: ospf
Name: Interface Tx Retransmit Type: Communications Alarm Probable cause: Hello	Severity: warning Object type: Interface Domain: ospf
Name: Lsdb Overflow Type: Equipment Alarm Probable cause: Resource Full	Severity: warning Object type: Site Domain: ospf
Name: Virtual Link Db Descript Auth Failure Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Virtual Link Domain: ospf
Name: Virtual Link Db Descript Config Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Virtual Link Domain: ospf
Name: Virtual Link Hello Auth Failure Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Virtual Link Domain: ospf
Name: Virtual Link Hello Config Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Virtual Link Domain: ospf
Name: Virtual Link Ls Ack Auth Failure Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Virtual Link Domain: ospf
Name: Virtual Link Ls Ack Config Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Virtual Link Domain: ospf
Name: Virtual Link Ls Req Auth Failure Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Virtual Link Domain: ospf
Name: Virtual Link Ls Req Config Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Virtual Link Domain: ospf
Name: Virtual Link Ls Update Auth Failure Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Virtual Link Domain: ospf

(5 of 12)

Alarm name, type, and default probable cause	Severity, object type, and domain
Name: Virtual Link Ls Update Config Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Virtual Link Domain: ospf
Name: Virtual Link Null Packet Auth Failure Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Virtual Link Domain: ospf
Name: Virtual Link Null Packet Config Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Virtual Link Domain: ospf
Name: Virtual Link Rx Bad Packet Type: Communications Alarm Probable cause: Hello	Severity: warning Object type: Virtual Link Domain: ospf
Name: Virtual Link Tx Retransmit Type: Communications Alarm Probable cause: Hello	Severity: warning Object type: Virtual Link Domain: ospf
Name: Default Instance Inconsistency Type: Configuration Alarm Probable cause: Multiple Default Instances Encountered	Severity: warning Object type: Manager Domain: policy
Name: Group Down Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Group Domain: rip
Name: Rip Authentication Failure Type: Authentication Alarm Probable cause: Auth Failure	Severity: warning Object type: Interface Domain: rip
Name: Rip Authentication Mismatch Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Interface Domain: rip
Name: Rip Down Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Site Domain: rip
Name: Rsvp Down Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Site Domain: rsvp
Name: Session Down Type: Protocol Alarm Probable cause: Interface Down	Severity: critical Object type: Session Domain: rsvp
Name: Mediation Authentication Failure Type: Communications Alarm Probable cause: Unsupported Sec Level	Severity: warning Object type: Mediation Policy Domain: security
Name: Management Access Filter Misconfigured Type: Configuration Alarm Probable cause: Invalid Source Port Identifier	Severity: warning Object type: Maf Entry Domain: sitesec

(6 of 12)

Alarm name, type, and default probable cause	Severity, object type, and domain
Name: Mediation Authentication Failure Type: Communications Alarm Probable cause: No Mediation Policy Found	Severity: critical Object type: Poller Manager Domain: snmp
Name: Ber Line Signal Degradation Type: Communications Alarm Probable cause: Ber Line Signal Degradation	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment
Name: Ber Line Signal Failure Type: Communications Alarm Probable cause: Ber Line Signal Failure	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment
Name: Line Alarm Indication Signal Type: Communications Alarm Probable cause: Line Alarm Indication Signal	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment
Name: Line Error Condition Type: Communications Alarm Probable cause: line Error Condition	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment
Name: Line Remote Defect Indication Type: Communications Alarm Probable cause: line Remote Defect Indication	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment
Name: Loss Of Clock Type: Communications Alarm Probable cause: Loss Of Clock	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment
Name: Path Alarm Indication Signal Type: Communications Alarm Probable cause: Path Alarm Indication Signal	Severity: major Object type: Sonet Channel Domain: sonetequipment
Name: Path B3 Error Type: Communications Alarm Probable cause: Path B3 Error	Severity: major Object type: Sonet Channel Domain: sonetequipment
Name: Path Loss Of Pointer Type: Communications Alarm Probable cause: Path Loss Of Pointer	Severity: major Object type: Sonet Channel Domain: sonetequipment
Name: Path Payload Mismatch Type: Communications Alarm Probable cause: path Payload Mismatch	Severity: major Object type: Sonet Channel Domain: sonetequipment
Name: Path Remote B3 Error Type: Communications Alarm Probable cause: path Remote B3 Error	Severity: major Object type: Sonet Channel Domain: sonetequipment
Name: Path Remote Defect Indication Type: Communications Alarm Probable cause: path Remote Defect Indication	Severity: major Object type: Sonet Channel Domain: sonetequipment
Name: Rx Section Synchronization Error Type: Communications Alarm Probable cause: Rx Section Synchronization Error	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment

(7 of 12)

Alarm name, type, and default probable cause	Severity, object type, and domain
Name: Section B1 Error Type: Communications Alarm Probable cause: Section B1 Error	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment
Name: Section Loss Of Frame Type: Communications Alarm Probable cause: section Loss Of Frame	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment
Name: Section Loss Of Signal Type: Communications Alarm Probable cause: section Loss Of Signal	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment
Name: Section S1 Failure Type: Communications Alarm Probable cause: section S1 Failure	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment
Name: Tx Section Synchronization Error Type: Communications Alarm Probable cause: Tx Section Synchronization Error	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment
Name: Frame Size Problem Type: Configuration Alarm Probable cause: Frame Size Problem	Severity: warning Object type: Service Domain: svc
Name: Service Site Down Type: Service Alarm Probable cause: Site Down	Severity: critical Object type: Site Domain: svc
Name: Topology Misconfigured Type: Configuration Alarm Probable cause: Topology Misconfigured	Severity: critical Object type: Service Domain: svc
Name: Type Mismatch Type: Configuration Alarm Probable cause: Service Site Type Misconfigured	Severity: critical Object type: Service Domain: svc
Name: Circuit Down Type: Circuit Alarm Probable cause: circuit Not Ready	Severity: critical Object type: Circuit Domain: svt
Name: Frame Size Problem Type: Configuration Alarm Probable cause: frame Size Problem	Severity: critical Object type: Circuit Domain: svt
Name: Keep Alive Problem Type: Oam Alarm Probable cause: keep Alive Failed	Severity: warning Object type: Tunnel Domain: svt
Name: Label Problem Type: Circuit Alarm Probable cause: label Problem	Severity: critical Object type: Circuit Domain: svt
Name: Tunnel Down Type: Path Alarm Probable cause: tunnel Down	Severity: critical Object type: Tunnel Domain: svt

(8 of 12)

Alarm name, type, and default probable cause	Severity, object type, and domain
Name: Boot Environment Sync Failed Type: Equipment Alarm Probable cause: boot Environment Sync Failed	Severity: critical Object type: Backup Restore Manager Domain: sw
Name: Bootable Config Backup Failed Type: Configuration Alarm Probable cause: file TransferF ailure	Severity: major Object type: Backup Restore Manager Domain: sw
Name: Bootable Config Restore Failed Type: Configuration Alarm Probable cause: file Transfer Failure	Severity: major Object type: Backup Restore Manager Domain: sw
Name: Config File Sync Failed Type: Equipment Alarm Probable cause: config File Sync Failed	Severity: critical Object type: Backup Restore Manager Domain: sw
Name: Hardware Boot Failure Type: Software Alarm Probable cause: software Boot Problem Due To Hardware Issues	Severity: critical Object type: Card Software Domain: sw
Name: Save Config Failed Type: Configuration Alarm Probable cause: file Access Error	Severity: major Object type: Backup Restore Manager Domain: sw
Name: Software Boot Failure Type: Software Alarm Probable cause: software Boot Problem	Severity: major Object type: Card Software Domain: sw
Name: Software Downloading Type: Aofware Alarm Probable cause: software Downloading	Severity: warning Object type: Card Software Domain: sw
Name: Software Initialized Type: Software Alarm Probable cause: software Initialized	Severity: warning Object type: Card Software Domain: sw
Name: Software Initializing Type: Software Alarm Probable cause: software Initializing	Severity: warning Object type: Card Software Domain: sw
Name: Software Upgrade Failed Type: Configuration Alarm Probable cause: file Access Error	Severity: major Object type: Backup Restore Manager Domain: sw
Name: DS1E1 Alarm Indication Signal Type: Communications Alarm Probable cause: alarm Indication Signal	Severity: major Object type: DS1E1 Channel Specifics Domain: tdmequipment
Name: DS1E1 Loss Of Frame Type: Communications Alarm Probable cause: loss Of F rame	Severity: major Object type: DS1E1 Channel Specifics Domain: tdmequipment
Name: DS1E1 Resource Availability Indicator Type: Communications Alarm Probable cause: resource Availability Indicator	Severity: major Object type: DS1E1 Channel Specifics Domain: tdmequipment

(9 of 12)

Alarm name, type, and default probable cause	Severity, object type, and domain
Name: DS3E3 Alarm Indication Signal Type: Communications Alarm Probable cause: alarm Indication Signal	Severity: major Object type: DS3E3 Channel Specifics Domain: tdmequipment
Name: DS3E3 Loss Of Signal Type: Communications Alarm Probable cause: loss Of Signal	Severity: major Object type: DS3E3 Channel Specifics Domain: tdmequipment
Name: DS3E3 Out Of Frame Type: Communications Alarm Probable cause: out Of Frame	Severity: major Object type: DS3E3 Channel Specifics Domain: tdmequipment
Name: Undefined Scheduler Reference Type: Configuration Alarm Probable cause: undefined Scheduler Reference	Severity: warning Object type: Service Type Definition Domain: vs
Name: Circuit Down Type: Circuit Alarm Probable cause: circuit Not Read	Severity: critical Object type: Circuit Domain: svt
Name: Frame Size Problem Type: Configuration Alarm Probable cause: frame Size Problem	Severity: critical Object type: Circuit Domain: svt
Name: Keep Alive Problem Type: OAM Alarm Probable cause: keep Alive Failed	Severity: warning Object type: Circuit Domain: svt
Name: Label Problem Type: Circuit Alarm Probable cause: label Problem	Severity: critical Object type: Circuit Domain: svt
Name: Tunnel Down Type: Path Alarm Probable cause: tunnel Down	Severity: critical Object type: Tunnel Domain: svt
Name: Boot Environment Sync Failed Type: Equipment Alarm Probable cause: boot Environment Syn Failed	Severity: critical Object type: Backup Restore Manager Domain: sw
Name: Bootable Config Backup Failed Type: Configuration Alarm Probable cause: file Transfer Failure	Severity: major Object type: Backup Restore Manager Domain: sw
Name: Bootable Config Restore Failed Type: Configuration Alarm Probable cause: file Transfer Failure	Severity: major Object type: Backup Restore Manager Domain: sw
Name: Config File Sync Failed Type: Equipment Alarm Probable cause: config File Sync Failed	Severity: critical Object type: Backup Restore Manager Domain: sw
Name: Hardware Boot Failure Type: Software Alarm Probable cause: software Boot Problem Due To Hardware Issues	Severity: critical Object type: Card Software Domain: sw

(10 of 12)

Alarm name, type, and default probable cause	Severity, object type, and domain
Name: Primary Image Boot Failure Type: Configuration Alarm Probable cause: boot Option File Misconfigured	Severity: warning Object type: Card Software Domain: sw
Name: Save Config Failed Type: Configuration Alarm Probable cause: file Access Error	Severity: major Object type: Backup Restore Manager Domain: sw
Name: Software Boot Failure Type: Software Alarm Probable cause: software Boot Problem	Severity: major Object type: Card Software Domain: sw
Name: Software Downloading Type: Software Alarm Probable cause: software Downloading	Severity: warning Object type: Card Software Domain: sw
Name: Software Initialized Type: Software Alarm Probable cause: software Initialized	Severity: warning Object type: Card Software Domain: sw
Name: Software Initializing Type: Software Alarm Probable cause: software Initializing	Severity: warning Object type: Card Software Domain: sw
Name: Software Redundancy Alert Type: Software Alarm Probable cause: secondary Status Change	Severity: warning Object type: Control Processor Software Domain: sw
Name: Software Redundancy Failure Alarm Type: Software Alarm Probable cause: restore Failed	Severity: major Object type: Control Processor Software Domain: sw
Name: Software Upgrade Failed Type: Configuration Alarm Probable cause: file Access Error	Severity: major Object type: Backup Restore Manager Domain: sw
Name: DS1E1 Alarm Indications Signal Type: Communications Alarm Probable cause: alarm Indications Signal	Severity: major Object type: DS1E1 Channel Specifics Domain: tdmequipment
Name: DS1E Looped Type: Communications Alarm Probable cause: far End Loopback	Severity: major Object type: DS1E1 Channel Specifics Domain: tdmequipment
Name: DS1E Loss Of Signal Type: Communications Alarm Probable cause: loss Of Signal	Severity: major Object type: DS1E1 Channel Specifics Domain: tdmequipment
Name: DS1E1 Out Of Frame Type: Communications Alarm Probable cause: out Of Frame	Severity: major Object type: DS1E1 Channel Specifics Domain: tdmequipment
Name: DS1E1 Resource Availability Indicator Type: Communications Alarm Probable cause: resource Availability Indicator	Severity: major Object type: DS1E1 Channel Specifics Domain: tdmequipment

(11 of 12)

Alarm name, type, and default probable cause	Severity, object type, and domain
Name: DS3E Alarm Indication Signal Type: Communications Alarm Probable cause: alarm Indication Signal	Severity: major Object type: DS3E3 Channel Specifics Domain: tdmequipment
Name: DS3E3 Looped Type: Communications Alarm Probable cause: far End Loopback	Severity: major Object type: DS3E3 Channel Specifics Domain: tdmequipment
Name: DS3E3 Loss Of Signal Type: Communications Alarm Probable cause: loss Of Signal	Severity: major Object type: DS3E3 Channel Specifics Domain: tdmequipment
Name: DS3E3 Out Of Frame Type: Communications Alarm Probable cause: out Of Frame	Severity: major Object type: DS3E3 Channel Specifics Domain: tdmequipment
Name: DS3E3 Resource Availability Type: Communications Alarm Probable cause: resource Availability Indicator	Severity: major Object type: DS3E3 Channel Specifics Domain: tdmequipment
Name: Undefined Scheduler Reference Type: Configuration Alarm Probable cause: undefined Scheduler Reference	Severity: warning Object type: Service Type Definition Domain: vs

(12 of 12)

29 — Troubleshooting and fault management using OAM

- 29.1 Troubleshooting and fault management using OAM overview 29-2**
- 29.2 Workflow to manage network faults using OAM tools 29-7**
- 29.3 Fault management OAM menus 29-8**
- 29.4 Fault management using OAM diagnostics procedures list 29-8**
- 29.5 Fault management using OAM diagnostics procedures 29-9**

29.1 Troubleshooting and fault management using OAM overview

The proper delivery of services requires a number of operations must occur correctly at different levels within the service creation model. For example, operations such as the association of packets to a service, VC labels to a service, and each service to a service tunnel (also called an SDP) 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 FIB information may cause connectivity issues.

To verify that a service is operational and that FIB information is correct, a set of configurable in-band or out-of-band, packet-based OAM tools are available. Each OAM diagnostic has the ability to test each of the individual packet operations.

For in-band, packet-based testing, the OAM packets closely resemble customer packets to effectively test the customer's forwarding path. However, these packets are distinguishable from customer packets, so they are kept within the service provider's network and not forwarded to the customer. For out-of-band testing, OAM packets are sent across some portion of the transport network. For example, across LSPs to test reachability.

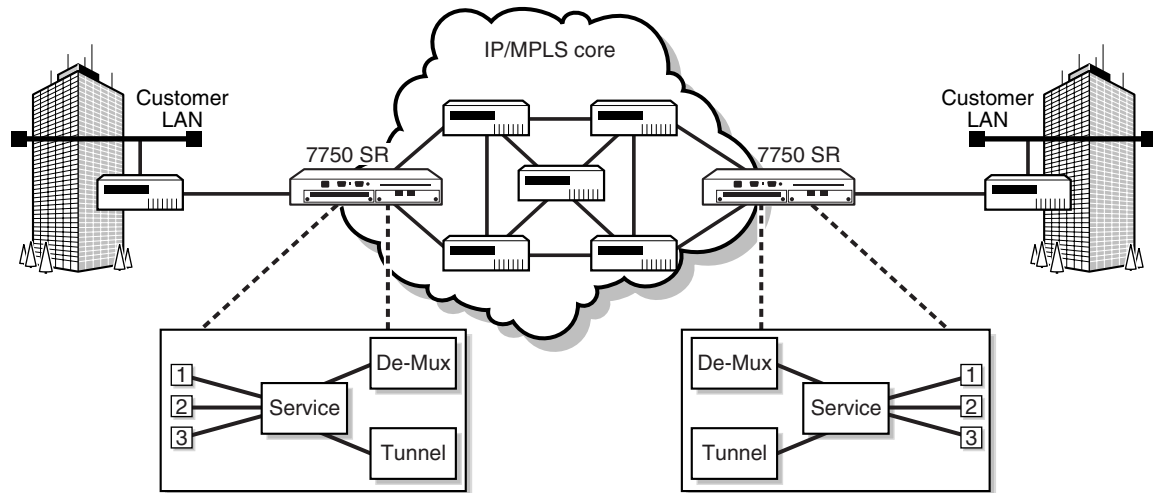
The following diagnostic tools are supported by the 5620 SAM:

- MTU OAM
- tunnel OAM
- circuit OAM
- LSP ping OAM
- LSP trace OAM
- MAC ping OAM
- MAC trace OAM
- MAC populate OAM
- MAC purge OAM
- VPRN ping
- VPRN trace

MTU and tunnel OAM diagnostics can be performed from both the service tunnel and from the service instance. Circuit OAM can only be performed from the service instance. MAC-level diagnostics can be performed from the circuits tab of the subscriber, service, or service site configuration forms. LSP diagnostics can be performed from the LSP manager.

Figure 29-1 shows how OAM troubleshooting tools can be used to fix service problems. A tunnel OAM packet can be inserted to test the connectivity between two customer LANs across the IP/MPLS core.

Figure 29-1 Sample OAM diagnostic



17228

MTU ping OAM

The MTU ping OAM diagnostic, which is called an `sdp-mtu` in the CLI, provides a tool for service providers to determine the exact frame size that is supported between the service ingress and service egress termination points, to within one byte. Use the MTU ping OAM to:

- determine the maximum frame size supported
- solve troubleshooting issues that are related to equipment used across the network core which may not be able to handle large frame sizes

In a large network, network devices can support a variety of packet sizes that are transmitted across its interfaces. This capability is referred to as the Maximum Transmission Unit (MTU) of network interfaces. You must consider the MTU of the entire path end-to-end when you provision services, especially for VLL services where the service must support the ability to transmit the largest customer packet.

Tunnel ping OAM

The Tunnel ping OAM, which is called an `sdp ping` in the CLI, performs in-band unidirectional or bidirectional connectivity tests on service tunnels. 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 size specified goes to the far-end IP address of the service tunnel ID within its encapsulation
- forwarding class mapping to ensure the test packet is treated the same as the customer traffic

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.

Circuit ping OAM

The Circuit ping OAM diagnostic, which is an `srv ping` in the CLI, provides end-to-end connectivity testing for an individual service. This diagnostic operates at a higher level than the tunnel OAM, 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 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 circuit ping OAM:

- verification that the local and remote service exists
- verification of the current state of the local and remote service
- ensuring that the local and remote service types are correlated
- ensuring that the same customer is associated with the local and remote service
- ensuring that there is a service to circuit association with both the local and remote service
- verification that the local and remote ingress and egress service labels match

LSP ping OAM

The LSP ping OAM, which is called an `lsp-ping` in CLI, performs in-band LSP connectivity tests.

In an LSP ping OAM, 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.

LSP trace OAM

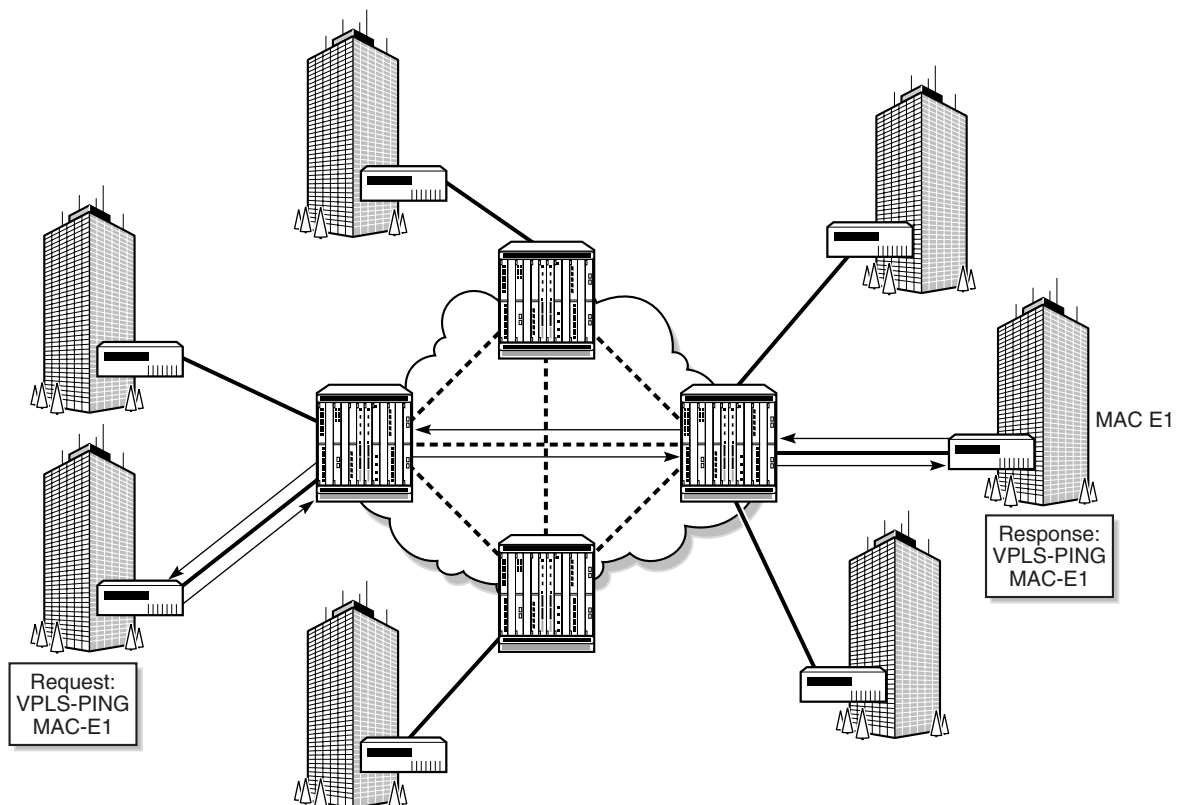
The LSP trace OAM, which is called an `lsp-trace` in CLI, displays the hop-by-hop route used by the LSP.

In an LSP trace OAM, the originating router creates an MPLS echo request packet for the LSP to be tested. The packet contains increasing values of the TTL setting in the outermost label. 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.

MAC ping OAM

The MAC ping OAM, which is called a mac-ping in CLI, is used to test connectivity in a VLL or VPLS service by verifying a remote MAC address. Figure 29-2 shows a sample MAC ping from one end of a service to the far-end MAC address of the service.

Figure 29-2 Sample MAC ping diagnostic



17246

The MAC ping OAM 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 OAM that is out-of-band, the ping is forwarded along the flooding domain when no MAC address bindings exist, or are 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 OAM 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.

MAC trace OAM

The MAC trace OAM, 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. 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 OAM 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 OAM 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.

MAC populate OAM

The MAC populate OAM, which is called `mac-populate` in CLI, is used to populate 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. 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 OAM, 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 the same OAM-tagged entry is added to the FIB tables of other devices.

MAC purge OAM

The MAC purge OAM, 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.

VPRN ping and VPRN trace

The VPRN ping and VPRN trace OAM are enabled from the VRF site of the subscriber's VPRN service. The VPRN ping OAM determines the existence of the far-end egress point of the service. VPRN pings can be sent in-band or out-of-band. The VPRN trace OAM displays the hop-by-hop route used to reach the target address at the far-end. VPRN traces can be sent in-band or out-of-band.

The general steps are:

- 1 Enable OAM from the VFF site of the subscriber's service by clicking on the Enable OAM button of the service configuration form's Site tab button.
- 2 Click on the Maintenance tab of the service configuration form.
- 3 To ping the VRF of a site in the VPN, enter the router ID.
- 4 Set the OAM test parameters.
- 5 Trigger the OAM diagnostic.
- 6 View the OAM results.

VPRN ping results are available from the History and Faults tabs. VPRN trace results are available from the History, Faults, and L3 Map tabs.

29.2 Workflow to manage network faults using OAM tools

- 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 Enable OAM for the site or service.

- 4 When the creation of a tunnel needs to be tested, or a customer service is compromised, use the OAM tools to troubleshoot the problem.
 - i Use the MTU ping OAM 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.
 - ii Use the tunnel ping OAM 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.
 - iii Use the circuit ping OAM to troubleshoot and resolve service problems that are related to the end-to-end connectivity of a customer service within the provider network.
 - iv Use the LSP ping and LSP trace OAM to troubleshoot and resolve problems that are related to MPLS LSPs.
 - v Use the MAC ping, MAC trace, MAC populate, and MAC purge OAM to troubleshoot and resolve problems that are related to FIBs and MAC addressing.
 - vi Use the VPRN ping and VPRN trace to troubleshoot and resolve problems with a VPRN service.
- 5 Use the OAM tool diagnostic response messages and history records to resolve the customer service problem.

29.3 Fault management OAM menus

Table 29-1 lists the OAM menus and their function.

Table 29-1 5620 SAM OAM menus

Menu option	Function
Topology→Service Tunnel Manager	Search for and open a service tunnel, and use the OAM tools to ensure that the GRE or MPLS transport network topology is valid.
Service Management→Browse Services	Search for and open the service, site, or subscriber that is compromised, and use the OAM tools to troubleshoot the service.

29.4 Fault management using OAM diagnostics procedures list

Table 29-2 lists the procedures necessary to execute OAM tasks.

Table 29-2 5620 SAM OAM diagnostic procedures list

Procedure	Purpose
To perform OAM diagnostics from a service tunnel	Validate the GRE or MPLS transport network before services are created.
To perform OAM diagnostics from a service	Locate the compromised service and start the OAM diagnostic to troubleshoot and solve the service issue.
To interpret OAM diagnostic results	Interpret the data from the OAM diagnostic to determine the solution to the problem that compromised the GRE or MPLS transport network, or caused a service issue.

29.5 Fault management using OAM diagnostics procedures

Use the following procedures to perform OAM diagnostics.

Procedure 29-1 To perform OAM diagnostics from a service tunnel

- 1 Choose Topology→Service Tunnel Manager from the 5620 SAM main menu.

The Service Tunnel Manager form appears.

- 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 appears.

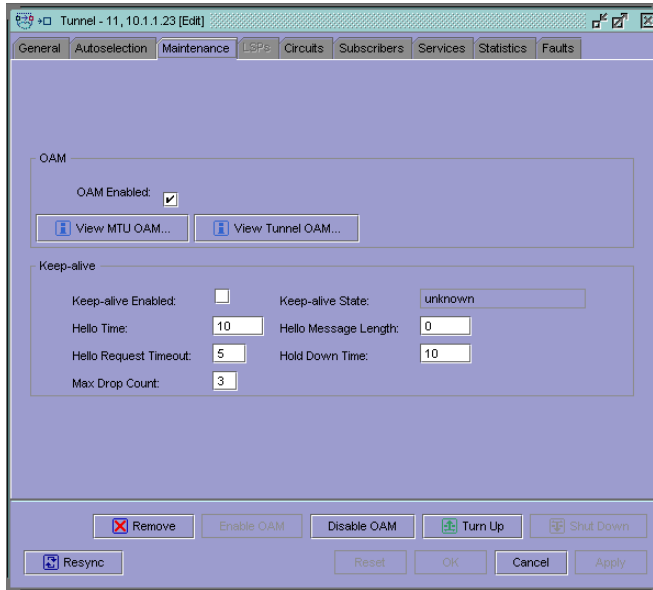
- 4 Click on the Maintenance tab button.

- 5 Select the OAM Enabled check box.

- 6 Click on the Apply button and confirm the action.

The View MTU Ping and View Tunnel Ping buttons are enabled, as shown in Figure 29-3.

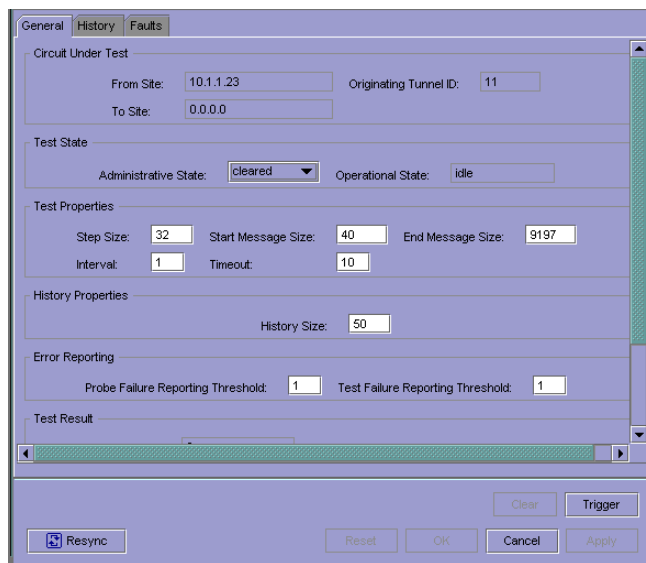
Figure 29-3 OAM form - Maintenance



- 7 Perform an MTU ping or Tunnel OAM diagnostic.
 - a Perform an MTU ping OAM diagnostic. Use the MTU diagnostic to find the largest valid frame size.
 - i Click on the View MTU Ping button.

The MTU Ping form appears with the General tab button selected, as shown in Figure 29-4. The form displays information about the circuit being tested, and the originating tunnel ID.

Figure 29-4 MTU ping form - General



- ii Configure the test properties.

The Start Message Size and the End Message Size parameters indicate the size of frame, in bytes, that is first tested, and the size of frame that ends the test. The Step Size parameter indicates by how many bytes the frame grows incrementally in size.



Note — If the step size is small, but the end message size is large, the amount of time to complete the MTU OAM diagnostic may be many minutes. Ensure that you have an appropriate step size that reflects the range of frame sizes you want to test.

- iii Click on the Apply button to save the changes.

- iv Confirm the action.

- v Click on the Trigger button.

The MTU ping diagnostic starts. The administrative state changes to reflect the status of the diagnostic. When the administrative state is done, the diagnostic is complete.

- vi Click on the History tab button.

The list of MTU ping OAM frames sent is displayed.

- vii Click on the row(s) as appropriate to view diagnostic information.

- viii Click on the Edit button.

The OAM history record form appears. The diagnostic information includes:

- source and destination of the diagnostic
- timestamp of when the test was completed
- time to complete the diagnostic, in seconds
- frame size sent
- OAM diagnostic status

See Procedure 29-3 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.

- ix Close the form.

- b Perform a Tunnel OAM diagnostic. Use the tunnel diagnostic to validate the GRE or MPLS transport network.

- i Click on the View Tunnel Ping button.

The Tunnel Ping form appears with the General tab button displayed, as shown in Figure 29-5. The form displays information about the circuit being tested, including the originating tunnel ID.

Figure 29-5 Tunnel ping form - General

The screenshot shows a web-based configuration interface for SdpOam. The window title is "SdpOam - 10.1.1.23, tr1-11 [Edit]". The interface has three tabs: "General", "History", and "Faults". The "General" tab is active and contains the following sections:

- Circuit Under Test:**
 - From Site: 10.1.1.23
 - To Site: 0.0.0.0
 - Originating Tunnel ID: 11
 - Return Tunnel ID: 0 (with a "Select..." button)
- Test State:**
 - Administrative State: cleared (dropdown menu)
 - Operational State: idle
- Test Properties:**
 - Probes to be Issued: 1
 - Message Size: 40
 - Forwarding Class: be (dropdown menu)
 - Profile: out (dropdown menu)
 - Interval: 1
 - Timeout: 10
- History Properties:**
 - History Size: 50
- Error Reporting:**
 - Probe Failure Reporting Threshold: 1
 - Test Failure Reporting Threshold: 1

At the bottom of the form, there are several buttons: "Resync" (with a refresh icon), "Clear", "Trigger", "Reset", "OK", "Cancel", and "Apply".

ii Configure the test properties.

- Configure the Return Tunnel ID parameter to specify the return tunnel, because the tunnels are unidirectional.
- Specify the Probes to be Issued parameter.
- Specify the Forwarding Class and Profile parameters. Ensure that the forwarding class is configured to work with the services planned to be sent across the tunnel.
- Set the Interval parameter only if you are sending multiple probes.

iii Click on the Apply button.

iv Confirm the action.

v Click on the Trigger button.

The Tunnel ping OAM diagnostic starts. The administrative state changes to reflect the diagnostic status. When the administrative state is done, the diagnostic is complete.

vi Click on the History tab button.

The tunnel test results are displayed.

vii Click on the row(s) as appropriate to view diagnostics information.

viii Click on the Edit button.

- iv You can perform a MAC Populate OAM diagnostic by clicking on the Populate MAC's button.
 - Click on the Populate MAC's button. The MAC Populate configuration form appears.
 - Set the Target MAC Address parameter, which is the MAC address.
 - Configure the Administrative State parameter to go to run the OAM diagnostic.
 - Configure the age for the request by setting the Age (seconds) parameter.
 - Select the force Oam check box to convert the MAC address to an OAM-generated MAC address, even if the MAC addresses was set by another method.
 - Select the flood check box to send the OAM MAC address to all upstream devices. Deselect the check box to send the OAM MAC address to the local FIB.
 - Select an access interface by clicking on the Select button next to the Sap Port parameter. Choose the port from the Select Port form, and click on the OK button.
 - Click on the Apply button.
 - Click on the Populate button to perform the OAM diagnostic.

- v You can perform a MAC Purge OAM diagnostic by clicking on the Purge MAC's button.
 - Click on the Purge MAC's button. The MAC Purge configuration form appears.
 - Set the Target MAC Address parameter, which is the MAC address to be purged.
 - Configure the Administrative State parameter to go to run the OAM diagnostic.
 - Select the Send via Control Plane check box to send the diagnostic packets via the control plane (in-band).
 - Select the Flood check box to purge the OAM MAC address from all upstream devices. Deselect the check box to purge the OAM MAC address from the local FIB.
 - Click on the Apply button.
 - Confirm the action.
 - Click on the Purge button to perform the OAM diagnostic.

- 5 Click on the Maintenance tab button.

The selected circuit(s) or site(s) for the service appears in the Circuit Ping, Tunnel Ping, MTU Ping, MAC Ping, MAC Trace, VPRN Ping, and VPRN Trace tab buttons, as shown in Figure 29-6.

- 6 Click on the Edit button to view previously generated diagnostics.

Figure 29-6 OAM configuration form from a service - MAC ping

Target MAC Address	Source MAC Address	Service ID	Service Name	From
FF-FF-FF-FF-FF-FF	6C-31-FF-00-00-01	1	VPLS service-1	38.120.182
FF-FF-FF-FF-FF-FF	6C-32-FF-00-00-01	1	VPLS service-1	38.120.182

- a View circuit ping OAM diagnostics from the Circuit Ping tab. When the diagnostic has been performed before, information about the diagnostic appears. Circuit ping OAM diagnostic information includes the:
- source and destination site IP addresses
 - administrative state
 - operational state
 - probes to be issued information
 - check mark buttons to specify whether a local test, remote test, or local and remote test is performed
 - information about previous circuit OAM diagnostics, including probes sent and responses received
 - ID of the service being diagnosed
 - name of the service being diagnosed

- b** View tunnel ping OAM diagnostics from the Tunnel Ping tab. See Procedure 29-1 for more information about performing a tunnel OAM diagnostic. When the diagnostic has been performed before, information about the diagnostic appears. Tunnel ping OAM diagnostic information includes the:

 - source and destination site IP addresses
 - originating and return tunnel IDs
 - administrative state
 - operational state
 - probes to be issued information
 - the message size
 - forwarding class used by the service
 - information about previous tunnel OAM diagnostics, including probes sent and responses received, the round trip time of the diagnostic test, and the average round trip time, in seconds
 - ID of the service being diagnosed
 - name of the service being diagnosed

- c** View MTU ping OAM diagnostics from the MTU Ping tab. See Procedure 29-1 for more information about performing an MTU ping OAM diagnostic. When the diagnostic has been performed before, information about the diagnostic appears. MTU ping OAM diagnostic information includes the:

 - source and destination site IP addresses
 - originating tunnel IDs
 - administrative and operational state
 - information about previous diagnostics, including the start and finish size of the MTU packet
 - ID of the service being diagnosed
 - name of the service being diagnosed

- d** View MAC ping diagnostics from the MAC Ping tab. When the diagnostic has been performed before, information about the diagnostic appears. MAC ping diagnostic information includes:

 - target and source MAC addresses
 - service ID and name
 - number of probes to be issued

- e** View MAC trace diagnostics from the MAC Trace tab. When the diagnostic has been performed before, information about the diagnostic appears. MAC trace diagnostic information includes:

 - target and source MAC addresses
 - service ID and name
 - number of probes to be issued

- f** View VPRN ping diagnostics from the VPRN Ping tab. When the diagnostic has been performed before, information about the diagnostic appears. VPRN ping diagnostic information includes:
- target and source IP addresses
 - service ID and name
 - number of probes to be issued
 - operational size
 - number of responses
- g** View VPRN trace diagnostics from the VPRN Trace tab. When the diagnostic has been performed before, information about the diagnostic appears. VPRN trace diagnostic information includes:
- target and source IP addresses
 - service ID and name
 - number of probes to be issued
 - operational size
 - number of responses
- 7** Select an OAM diagnostic from the appropriate tab.
- 8** Click on the Trigger button.
- 9** The OAM configuration form appears for the type of diagnostic you are performing.
- a** To perform an MTU ping OAM diagnostic, see step 7 of Procedure 29-1.
- b** To perform a tunnel ping OAM diagnostic, see step 7 of Procedure 29-1.
- c** Perform a circuit ping OAM diagnostic to ensure that customer traffic on the service is transmitted. Figure 29-7 shows a Circuit Ping form with the General tab button selected.

Figure 29-7 Circuit ping form - General

The screenshot shows a web-based configuration form for a circuit ping diagnostic. The form is titled "Circuit ping form - General" and has three tabs: "General", "History", and "Faults". The "General" tab is selected. The form contains several sections:

- Circuit Under Test:** Two text input fields for "From Site" (10.1.1.31) and "To Site" (10.1.1.30).
- Test State:** Two dropdown menus for "Administrative State" (set to "cleared") and "Operational State" (set to "idle").
- Test Properties:** Two checkboxes for "Test Local" and "Test Remote", both of which are checked.
- History Properties:** A text input field for "History Size" (set to 50).
- Error Reporting:** Two text input fields for "Probe Failure Reporting Threshold" and "Test Failure Reporting Threshold", both set to 1.
- Test Result:** A dropdown menu for "Status" (set to "undetermined"), and two text input fields for "Number Of Probes Sent" (0) and "Number Of Responses Received" (0).

At the bottom of the form, there are several buttons: "Resync" (with a refresh icon), "Clear", "Trigger", "Reset", "OK", "Cancel", and "Apply".

- i Click on the Circuit Ping tab.
A list of circuits appears.
 - ii Double-click on a circuit in the list.
The Circuit Ping configuration form appears.
 - iii Configure the parameters of the circuit ping OAM test of a service:
 - specify whether to test the local IP address, the far-end IP address, or both IP addresses using the Test Local and Test Remote check boxes
 - configure the error reporting thresholds
 - iv Click on the Apply button.
 - v Confirm the action.
 - vi Click on the Trigger button.

The circuit ping OAM diagnostic is performed. See Procedure 29-3 for more information about the diagnostic status messages. Use the status message to interpret the diagnostic results.
- d To perform an MAC ping OAM diagnostic:
- i Click on the MAC Ping tab.
A list of MAC addresses appears.
 - ii Double-click on a row in the list.
The OAM diagnostic configuration form appears.
 - iii Configure the parameters from the appropriate tabs. Table 29-3 list the MAC ping parameters.

Table 29-3 MAC ping parameters

Parameter	Options and description
Target MAC Address	The MAC address for the destination address in MAC notation. You can target the MAC broadcast address of FF-FF-FF-FF-FF-FF in the data plane to flood the service domain and receive a response from all operational service access ports. No response is received from a MAC ping on the broadcast address performed via the control plane.
Source MAC Address	The MAC address for the source address is in MAC notation.
Administrative State	Choose go to enable the OAM diagnostic.
Probes to be Issued	The number of OAM packets to send. The range is 1 to 155.
Send on Control Plane	Select the check mark box to have the OAM request sent via the control plane.

(1 of 2)

Parameter	Options and description
Reply via Control Plane	Select the check mark box to have the OAM response arrive via the control plane.
Size	The size of the OAM packet, in octets.
Timeout	The amount of time that the 5620 SAM waits for a reply message after sending out the OAM packet. After the timeout period is exceeded, any response message is ignored.
Interval	The amount of time that must expire before the next OAM packet is sent. If the Probes to be Issued parameter is set to 1, no additional OAM packets are sent. When the Interval parameter is set to one second and the Timeout parameter is set to 10 seconds, the maximum time between message requests is 10 seconds, and the minimum time is one second.
History Size	The number of OAM request history records to store in the History tab.

(2 of 2)

- iv Click on the Apply button.
- v Confirm the action.
- vi Click on the Trigger button.

The MAC ping OAM diagnostic is performed. Use the status message and details in the History tab to interpret the diagnostic results.

- e To perform an MAC trace OAM diagnostic:
 - i Click on the MAC Trace tab.
A list of MAC addresses appears.
 - ii Double-click on a row in the list.
The OAM diagnostic configuration form appears.
 - iii Configure the parameters from the appropriate tabs. Table 29-4 lists the MAC trace parameters.

Table 29-4 MAC trace parameters

Parameter	Options and description
Target MAC Address	The MAC address for the destination address is in MAC notation.
Source MAC Address	The MAC address for the source address is in MAC notation.
Administrative State	Choose go to enable the OAM diagnostic.
Probes per Hop	The number of OAM packets to send for a particular TTL value. The range is 1 to 155.

(1 of 2)

Parameter	Options and description
Send on Control Plane	Select the check mark box to have the OAM request sent via the control plane.
Reply via Control Plane	Select the check mark box to have the OAM response arrive via the control plane.
Size (octets)	The size of the OAM packet, in octets. The request packet size is padded to the specified size using a six-byte PAD header and a byte payload of 0xAA, as necessary.
Initial Timeout	The minimum TTL value in the VC label for the OAM trace. The range is 1 to 255.
Max Timeout	The maximum TTL value in the VC label for the OAM trace. The range is 1 to 255. The Max Timeout value must be greater than the Initial Timeout value.
Interval (seconds)	The amount of time before the next OAM packet is sent. If the Probes per Hop parameter is set to 1, no additional OAM packets are sent. When the Initial Timeout parameter is set to one second and the Max Timeout parameter is set to 10 s, the maximum time between message requests is 10 s, and the minimum time is one second.
History Size	The number of OAM request history records to store in the History tab

(2 of 2)

- iv Click on the Apply button.
- v Confirm the action.
- vi Click on the Trigger button.

The MAC trace OAM diagnostic is performed. Use the status message and details in the History tab to interpret the diagnostic results.

- f To perform an VPRN ping OAM diagnostic:
 - i Click on the VPRN Ping tab.
A list of VPRN services appears.
 - ii Double-click on a row in the list.
The OAM diagnostic configuration form appears.
 - iii Configure the parameters from the appropriate tabs. Table 29-5 lists the parameters.

Table 29-5 VPRN ping parameters

Parameter	Options and description
Target Address	The IP address for the destination address in IP dotted decimal notation
Source Address	The IP address for the source address in IP dotted decimal notation
Administrative State	Choose go to enable the OAM diagnostic.
Probes to be Issued	The number of OAM packets to send. The range is 1 to 155.
Label TTL	The time to live (TTL) value in the VC label for the OAM request, expressed as a decimal. The range is 1 to 255.
Reply via Control Plane	Select the check mark box to have the OAM response arrive via the control plane.
Size (octets)	The size of the OAM packet, in octets.
Timeout (seconds)	The amount of time that the 5620 SAM waits for a reply message after sending out the OAM packet. After the timeout period is exceeded, any response message is ignored.
Interval (seconds)	The amount of time that must expire before the next OAM packet is sent. If the Probes to be Issued parameter is set to 1, no additional OAM packets are sent. When the Interval (seconds) parameter is set to one second and the Timeout (seconds) parameter is set to 10 seconds, the maximum time between message requests is 10 seconds, and the minimum time is one second.
History Size	The number of OAM request history records to store in the History tab.

- iv Click on the Apply button.
- v Confirm the action.
- vi Click on the Trigger button.

The VPRN ping OAM diagnostic is performed. Use the status message and details in the History tab to interpret the diagnostic results.

- g To perform an VPRN trace OAM diagnostic:
 - i Click on the VPRN Trace tab.
A list of VPRN services appears.
 - ii Double-click on a row in the list.
The OAM diagnostic configuration form appears.
 - iii Configure the parameters from the appropriate tabs. Table 29-6 lists the VPRN trace parameters.

Table 29-6 VPRN trace parameters

Parameter	Options and description
Target Address	The IP address for the destination address in IP dotted decimal notation
Source Address	The IP address for the source address in IP dotted decimal notation
Administrative State	Choose go to enable the OAM diagnostic.
Probes per Hop	The number of OAM packets to send for a particular TTL value. The range is 1 to 155.
Reply via Control Plane	Select the check mark box to have the OAM response arrive via the control plane.
Size (octets)	The size of the OAM packet, in octets.
Initial Timeout	The minimum TTL value in the VC label for the OAM trace. The range is 1 to 255.
Maximum Timeout	The maximum TTL value in the VC label for the OAM trace. The range is 1 to 255. The Maximum Timeout value must be greater than the Minimum Timeout value.
Interval (seconds)	The amount of time that must expire before the next OAM packet is sent. If the Probes to be Issued parameter is set to 1, no additional OAM packets are sent. When the Initial Timeout parameter is set to one second and the Maximum Timeout parameter is set to 10 s, the maximum time between message requests is 10 s, and the minimum time is one second.
History Size	The number of OAM request history records to store in the History tab

- iv Click on the Apply button.
- v Confirm the action.
- vi Click on the Trigger button.

The VPRN trace OAM diagnostic is performed. Use the status message and details in the History tab to interpret the diagnostic results.

- 10 Click on the Close button.

Procedure 29-3 To interpret OAM diagnostic results

- 1 Perform the OAM diagnostic, as described in Procedures 29-1 and 29-2.
- 2 View the OAM diagnostic history results from the History tab, or the information presented in the OAM diagnostic General tab.
- 3 The status field displays the key information about OAM diagnostic results.

- 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 29-7 lists the displayed messages and a description.

Table 29-7 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 circuit OAM diagnostics, the key information is the result of the diagnostic, which is displayed in the status message and with the other records in the History tab.

As the diagnostic traverses the service across the originating and destination IP address, the service tunnels, and the used VCs, the status of each portion of the service is displayed. Table 29-8 lists the displayed messages and a description.

Table 29-8 Circuit 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 and VPRN ping OAM diagnostics, the key information is the result of the diagnostic. Table 29-9 lists the displayed messages, the return code, and a description.

Table 29-9 MAC and VPRN 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 given 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.
tlvNotUnderstood (9)	One or more TLVs were not understood.

Performance monitoring using statistics

30 — Accounting and performance monitoring using statistics

30 — Accounting and performance monitoring using statistics

- 30.1 Accounting and performance monitoring using statistics overview 30-2**
- 30.2 Workflow for statistics collection 30-18**
- 30.3 Statistics menus 30-19**
- 30.4 Statistics procedure list 30-19**
- 30.5 Performance monitoring using statistics procedures 30-20**

30.1 Accounting and performance monitoring using statistics overview

Performance monitoring and accounting statistics collection is performed on the 5620 SAM using service- and equipment-related statistics counters from the managed devices. There are two types of statistics collected:

- service access points and network ports for accounting statistics, which can be used for billing and traffic analysis purposes
- network object performance statistics, for control plane, data forwarding plan, and device utilization statistics

The benefits of statistics collection from the 5620 SAM are:

- equipment statistics monitoring in near-real time
- service-based enforcement of SLAs
- detailed accounting statistics for billing
- detailed control of statistics collection counters, collection intervals, and application to network objects

Accounting

Service access point accounting statistics are used to measure usage on each service queue, which can be rolled up for billing. These accounting records can be used to determine customer service usage, and to feed into a billing application. Network port statistics are used to measure usage within each forwarding class queue, as defined on the network port. This information can be used to track link utilization and network traffic patterns and trends to help capacity planning and traffic engineering efforts.

Statistics generated and stored on the devices are collected and transferred by FTP to the 5620 SAM based on user-configured collection intervals, or when a collection request is made.

All statistics are collected within the counters of the individual service queues defined on the customer access port or the counters within forwarding classes queues defined on the network ports. By default, the accounting statistics are collected every five minutes for service ingress or service egress statistics. By default, the accounting statistics are collected every 15 minutes for combination service statistics.

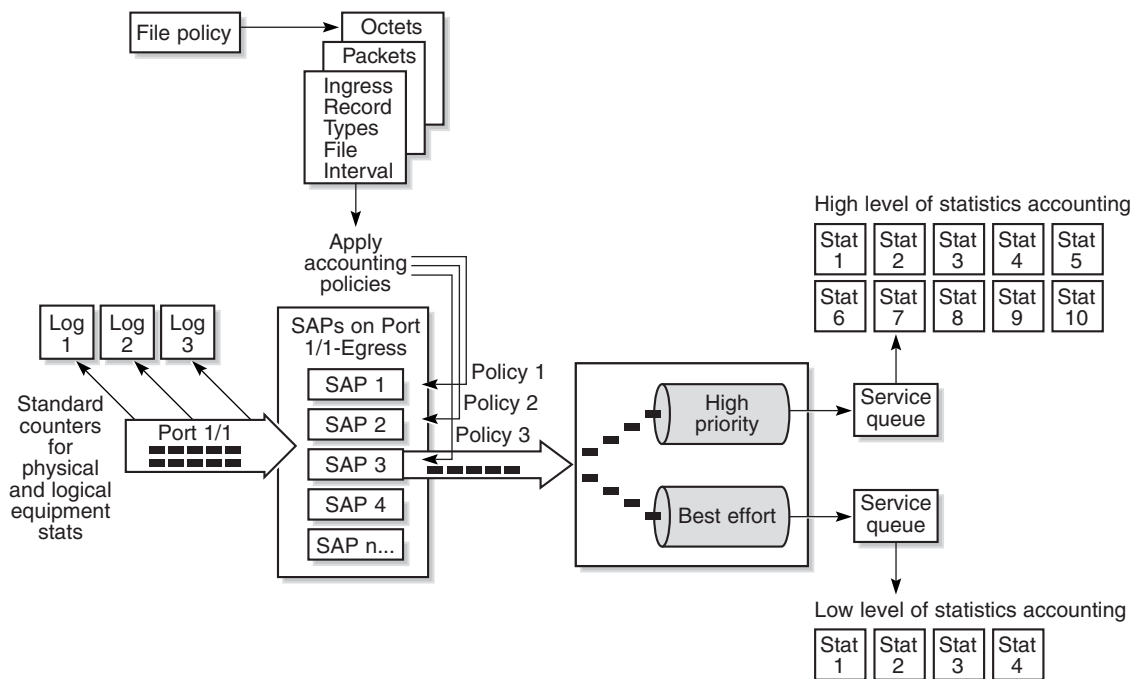
You can control how often the service access point statistical counters are collected and applied to all services. You can create accounting policies that determine which statistical classes, and counters within each class, are collected. The statistics types, the counters, and the information contained in the accounting records are listed in Table 30-1.

These policies can be applied to services, such as VPLS. The statistics generated and collected can then be used to:

- check throughput to confirm SLAs
- correlate data for billing
- monitor service quality

There can be a combinations of flat-rate, destination-based, or usage based billing. Figure 30-1 shows how accounting statistics policies are applied to services.

Figure 30-1 Accounting statistics policies applied to services



17185

As shown in Figure 30-1, there are different statistic policies applied to the services. The subscriber using service access point 3 on port 1/1 as a service egress point has two services, one high priority and one best effort. The statistics policies applied to each service type are different; for the high priority service, more statistics are collected than for the best effort service.

Performance monitoring

You can monitor equipment in near-real time using control plane, data forwarding plan, and device utilization performance statistics. Performance statistics counters are collected every 15 min by default against network ports. You can apply policies for each port if necessary, but the default counters should be sufficient.

Some of the types of statistics you can collect for equipment and logical objects are listed. When a network statistics collection policy is configured, counters are retrieved from the managed device MIBs using an SNMP getBulk command. For example, interface statistics correspond to the IF-MIB.

The following lists the types of network performance statistics you can collect. See Table 30-2 for a complete list of all performance statistical counter types collected per package and MIB type.

- Access Interface Stp Stats
- Area Basic Stats
- Area Interface Stats
- Area Lsa Stats
- Dot 3 stats
- Dynamic Lsp Stats
- Ethernet Stats
- Interface Stats
- Tunnel Stats
- Virtual Neighbor Stats
- Virtual Link Stats
- LSP Stats
- Media Independence Stats
- Mpls Stats
- Neighbor Stats
- Peer Stats
- Ppp Stats
- Route Stats
- Rsvp Stats
- Site Stats
- SONET Stats
- Virtual Neighbor Stats

Statistical policies, values, and counters

The following lists the main elements of an accounting statistics record.

- Identifiers specify the physical or logical object against which statistics are collected.
- Accounting policy type, also called billing records, defines the class of statistics. There are two main classes: network and access.
- Statistics classes, also called records or counters, define the detailed collection of statistics information from the managed devices.

Table 30-1 lists the elements in an accounting statistics log record.

Table 30-1 Accounting statistics log record information

Accounting policy type	Description	Possible values
Default identifiers for network and access records	<ul style="list-style-type: none"> • Timestamp indicates when the record was collected • The information necessary to identify the object against which the statistics were collected, for example service ID 10, access port 1/1/2:0, and queue ID 1 	<p>For service-related statistics IDs:</p> <ul style="list-style-type: none"> • timestamp • suspect if the entry may not contain correct data • poll information, either scheduled resynchronization or manual resynchronization • router ID • data svc = service ID • sap = service access port • qid = queue ID <p>For network-related statistics IDs:</p> <ul style="list-style-type: none"> • timestamp • suspect if the entry may not contain correct data • poll information, either scheduled resynchronization or manual resynchronization • router ID • port = network port ID • fc = forwarding class
Accounting policy class	The type of statistic class collected at the beginning and the end of the log record	<p>service ingress octets (record # 1, abbreviation sio) service egress octets (record # 2, abbreviation seo) service ingress packets (record # 3, abbreviation sip) service egress packets (record # 4, abbreviation sep) network ingress octets (record # 5, abbreviation nio) network egress octets (record # 6, abbreviation neo) network ingress packets (record # 7, abbreviation nip) network egress packets (record # 8, abbreviation nep) compact service ingress octets (record # 9, abbreviation ctSio) combined service ingress (record # 10, abbreviation ctSipo) combined network ing egr octets (record # 11, abbreviation cmNio and cmNeo) combined service ing egr octets (record # 12, abbreviation cmSio and cmSeo) complete service ingress egress (record # 13, abbreviation cmSipo and cmSepso)</p>

(1 of 2)

Accounting policy type	Description	Possible values
Statistics classes, the individual counter and its value	<p>The type of statistic collected and the value of the statistical counter in the collection interval.</p> <p>See the appropriate user documentation or contact your Alcatel support representative for a complete list of statistics.</p>	<p>The type of statistics collected for each statistics class varies.</p> <p>Some service-related statistics:</p> <ul style="list-style-type: none"> • loo = low octets offered • hpd = high packets dropped • ipf = in profile packets forwarded <p>Some network-related statistics:</p> <ul style="list-style-type: none"> • iof = in profile octets forwarded • opd = out of profile packets dropped
	service ingress octets	<ul style="list-style-type: none"> • hoo = high octets offered • hod = high octets dropped • loo = low octets offered • lod = low octets dropped • iof = in profile octets forwarded • oof = out of profile octets forwarded
	service egress octets network egress octets	<ul style="list-style-type: none"> • iof = in profile octets forwarded • iod = in profile octets dropped • oof = out of profile octets forwarded • ood = out of profile octets dropped
	service ingress packets network ingress packets	<ul style="list-style-type: none"> • hpo = high packets offered • hpd = high packets dropped • lpo = low packets offered • lpd = low packets dropped • ipf = in profile packets forwarded • opf = out of profile packets forwarded
	service egress packets network egress packets	<ul style="list-style-type: none"> • ipf = in profile packets forwarded • ipd = in profile packets dropped • opf = out of profile packets forwarded • opd = out of profile packets dropped
	network ingress octets	<ul style="list-style-type: none"> • iof = in profile octets forwarded • iod = in profile octets dropped • oof = out of profile octets forwarded • ood = out of profile octets dropped
	compact service ingress octets	<ul style="list-style-type: none"> • hoo = high octets offered • hod = high octets dropped • loo = low octets offered • lod = low octets dropped
	combined service ingress packet octets	combined service ingress packets and service ingress octets
	combined network ingress egress octets	Combined network ingress octets and network egress octets
	combined service ingress egress octets	Combined service ingress octets and service egress octets
	complete service ingress packet octets	Combined service ingress packets and service ingress octets
	complete service egress packet octets	Combined service egress packets and service egress octets

(2 of 2)

Network statistics records can be found on the GUI from most physical equipment and logical element configuration forms. Use the information to:

- understand the parameters that comprise each of the statistical counters
- determine which MIB is the source of the statistical counter, for further investigation
- a description of the counter

Table 30-2 lists all available network performance statistical counters.

Table 30-2 Network performance statistical counters

Statistic counter name	Source MIB	Description
bgp.PeerStats		
flaps	TIMETRA-BGP-MIB.tBgpPeerOperEntry.tBgpPeerOperFlaps	Number of flaps of updates from this peer.
inputQueueMessages	TIMETRA-BGP-MIB.tBgpPeerOperEntry.tBgpPeerOperInputQueueMessages	Number of unprocessed messages in the queue, from this peer.
lastEvent	TIMETRA-BGP-MIB.tBgpPeerOperEntry.tBgpPeerOperLastEvent	Last BGP event of this peer.
lastState	TIMETRA-BGP-MIB.tBgpPeerOperEntry.tBgpPeerOperLastState	Last BGP state of this peer.
messageOctetsReceived	TIMETRA-BGP-MIB.tBgpPeerOperEntry.tBgpPeerOperMsgOctetsRcvd	Number of octets received from this peer.
messageOctetsSent	TIMETRA-BGP-MIB.tBgpPeerOperEntry.tBgpPeerOperMsgOctetsSent	Number of octets transmitted to this peer.
outputQueueMessages	TIMETRA-BGP-MIB.tBgpPeerOperEntry.tBgpPeerOperOutputQueueMessages	Number of untransmitted messages in the queue, to this peer.
pathsReceived	TIMETRA-BGP-MIB.tBgpPeerOperEntry.tBgpPeerOperReceivedPaths	Number of paths received from this peer.
pathsSuppressedByDamping	TIMETRA-BGP-MIB.tBgpPeerOperEntry.tBgpPeerOperPathsSuppressedByDamping	Number of paths from this peer, which have been suppressed by damping.
prefixesActive	TIMETRA-BGP-MIB.tBgpPeerOperEntry.tBgpPeerOperActivePrefixes	Number of active prefixes from this peer.
prefixesReceived	TIMETRA-BGP-MIB.tBgpPeerOperEntry.tBgpPeerOperReceivedPrefixes	Number of prefixes received from this peer.
prefixesSent	TIMETRA-BGP-MIB.tBgpPeerOperEntry.tBgpPeerOperSentPrefixes	Number of prefixes received from this peer.
vpnActivePrefixes	TIMETRA-BGP-MIB.tBgpPeerOperEntry.tBgpPeerOperVpnActivePrefixes	The number of active VPN prefixes from this BGP peer.

(1 of 12)

Statistic counter name	Source MIB	Description
vpnReceivedPrefixes	TIMETRA-BGP-MIB.tBgpPeerOperEntry.tBgpPeerOperVpnReceivedPrefixes	The number of received VPN prefixes.
vpnSentPrefixes	TIMETRA-BGP-MIB.tBgpPeerOperEntry.tBgpPeerOperVpnSentPrefixes	The number of transmitted VPN prefixes.
equipment.InterfaceAdditionalStats		
receivedBroadcastPackets	IF-MIB.ifXEntry.ifHCInBroadcastPkts	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer. This object is a 64-bit version of ifInBroadcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
receivedMulticastPackets	IF-MIB.ifXEntry.ifHCInMulticastPkts	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of ifInMulticastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
receivedTotalOctets	IF-MIB.ifXEntry.ifHCInOctets	The total number of octets received on the interface, including framing characters. This object is a 64-bit version of ifInOctets. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
receivedUnicastPackets	IF-MIB.ifXEntry.ifHCInUcastPkts	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer. This object is a 64-bit version of ifInUcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
statsIndex	IF-MIB.ifXEntry.ifIndex	A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization.

(2 of 12)

Statistic counter name	Source MIB	Description
transmittedBroadcastPackets	IF-MIB.ifXEntry.ifHCOOutBroadcastPkts	<p>The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of ifOutBroadcastPkts.</p> <p>Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
transmittedMulticastPackets	IF-MIB.ifXEntry.ifHCOOutMulticastPkts	<p>The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of ifOutMulticastPkts.</p> <p>Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
transmittedTotalOctets	IF-MIB.ifXEntry.ifHCOOutOctets	<p>The total number of octets transmitted out of the interface, including framing characters. This object is a 64-bit version of ifOutOctets.</p> <p>Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
transmittedUnicastPackets	IF-MIB.ifXEntry.ifHCOOutUcastPkts	<p>The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of ifOutUcastPkts.</p> <p>Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>
equipment.InterfaceStats		
outboundBadPackets	IF-MIB.ifEntry.ifOutErrors	<p>For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.</p> <p>Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.</p>

(3 of 12)

Statistic counter name	Source MIB	Description
outboundPacketsDiscarded	IF-MIB.ifEntry.ifOutDiscards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
receivedBadPackets	IF-MIB.ifEntry.ifInErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
receivedOctets	IF-MIB.ifEntry.ifInOctets	The total number of octets received on the interface, including framing characters. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
receivedPacketsDiscarded	IF-MIB.ifEntry.ifInDiscards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
receivedUnicastPackets	IF-MIB.ifEntry.ifInUcastPkts	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

(4 of 12)

Statistic counter name	Source MIB	Description
receivedUnknownProtocolPackets	IF-MIB.ifEntry.ifInUnknownProtos	For packet-oriented interfaces, the number of packets received via the interface which were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter will always be 0. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
statsIndex	IF-MIB.ifEntry.ifIndex	A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization.
transmittedOctets	IF-MIB.ifEntry.ifOutOctets	The total number of octets transmitted out of the interface, including framing characters. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
transmittedUnicastPackets	IF-MIB.ifEntry.ifOutUcastPkts	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
equipment.SystemCpuStats		
systemCpuUsage	TIMETRA-SYSTEM-MIB.sgiCpuUsage	The value of sgiCpuUsage specifies the current CPU utilization for the system.
equipment.SystemMemoryStats		
systemMemoryUsage	TIMETRA-SYSTEM-MIB.sgiMemoryUsed	The value of sgiMemoryUsed specifies the total memory currently in use by the software running on the system.
ospf.AreaBasicStats		
areaBorderRouterCount	OSPF-MIB.ospfAreaEntry.ospfAreaBdrRtrCount	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
autonomousSystemBorderRouterCount	OSPF-MIB.ospfAreaEntry.ospfAsBdrRtrCount	The total number of Autonomous System border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
nssaTranslatorEvents	OSPF-MIB.ospfAreaEntry.ospfAreaNssaTranslatorEvents	Indicates the number of Translator State changes that have occurred since the last boot-up.

(5 of 12)

Statistic counter name	Source MIB	Description
totalLSACount	OSPF-MIB.ospfAreaEntry.ospfAreaLsaCount	The total number of link-state advertisements in this area's link-state database, excluding AS External LSA's.
totalSpfRuns	OSPF-MIB.ospfAreaEntry.ospfSpfRuns	The number of times that the intra-area route table has been calculated using this area's link-state database. This is typically done using Dijkstra's algorithm.
ospf.AreaInterfaceStats		
activeInterfaces	TIMETRA-OSPF-MIB.vRtrOspfAreaEntry.vRtrOspfAreaActiveInterfaces	The total number of currently active interfaces in this area.
interfaces	TIMETRA-OSPF-MIB.vRtrOspfAreaEntry.vRtrOspfAreaInterfaceCount	The total number of interfaces configured in this area.
virtualInterfaces	TIMETRA-OSPF-MIB.vRtrOspfAreaEntry.vRtrOspfAreaVirtualLinkCount	The total number of virtual links configured through this area.
ospf.AreaLsaStats		
type10LSA	TIMETRA-OSPF-MIB.vRtrOspfAreaEntry.vRtrOspfAreaType10LsaCount	The total number of OSPF type 10 Link State Advertisements (LSAs) in this area.
type1LSA	TIMETRA-OSPF-MIB.vRtrOspfAreaEntry.vRtrOspfAreaType1LsaCount	The total number of OSPF Type 1 Link State Advertisements (LSAs) in this area.
type2LSA	TIMETRA-OSPF-MIB.vRtrOspfAreaEntry.vRtrOspfAreaType2LsaCount	The total number of OSPF Type 2 Link State Advertisements (LSAs) in this area.
type3LSA	TIMETRA-OSPF-MIB.vRtrOspfAreaEntry.vRtrOspfAreaType3LsaCount	The total number of OSPF Type 3 Link State Advertisements (LSAs) in this area.
type4LSA	TIMETRA-OSPF-MIB.vRtrOspfAreaEntry.vRtrOspfAreaType4LsaCount	The total number of OSPF Type 4 Link State Advertisements (LSAs) in this area.
type7LSA	TIMETRA-OSPF-MIB.vRtrOspfAreaEntry.vRtrOspfAreaType7LsaCount	The total number of OSPF Type 7 Link State Advertisements (LSAs) in this area.
ospf.InterfaceGeneralStats		
events	OSPF-MIB.ospfIfEntry.ospfIfEvents	The number of times this OSPF interface has changed its state, or an error has occurred.
lsaCount	OSPF-MIB.ospfIfEntry.ospfIfLsaCount	The total number of link-local link state advertisements in this interface's link-local link state database.
ospf.InterfaceNeighborStats		
neighborCount	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfNeighborCount	The total number of OSPF neighbors adjacent on this interface, in a state of INIT or greater, since ospfAdminStat was last set to 'enabled'.
ospf.InterfaceReceiveStats		

(6 of 12)

Statistic counter name	Source MIB	Description
databaseDescriptionPackets	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfRxDBDs	The total number of OSPF DataBase Description packets received on this interface since ospfAdminStat was last set to 'enabled'.
helloPackets	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfRxHello	The total number of OSPF Hello packets received on this interface since ospfAdminStat was last set to 'enabled'.
linkStateAcknowledgements	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfRxLSAcks	The total number of Link State Acknowledgements received on this interface since ospfAdminStat was last set to 'enabled'.
linkStateRequests	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfRxLSRs	The total number of Link State Requests (LSRs) received on this interface since ospfAdminStat was last set to 'enabled'.
linkStateUpdates	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfRxLSUs	The total number of Link State Updates (LSUs) received on this interface since ospfAdminStat was last set to 'enabled'.
totalPackets	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfRxPackets	The total number of OSPF packets received on this interface since ospfAdminStat was last set to 'enabled'.
ospf.InterfaceStatusStats		
authorizationFailures	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfAuthFailures	The total number of OSPF packets received with an invalid authorization key since ospfAdminStat was last set to 'enabled'.
badAreas	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfBadAreas	The total number of OSPF packets received with an area mismatch since ospfAdminStat was last set to 'enabled'.
badAuthorizationTypes	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfBadAuthTypes	The total number of OSPF packets received with an invalid authorization type since ospfAdminStat was last set to
badDeadIntervals	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfBadDeadIntervals	The value of vRtrOspfIfBadDeadIntervals is the total number of OSPF packets received where the dead interval given in the packet was not equal to that configured on this interface since ospfAdminStat was last set to 'enabled'.
badDestinationAddresses	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfBadDstAdrs	The total number of OSPF packets received with the incorrect IP destination address since ospfAdminStat was last set to
badHelloIntervals	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfBadHelloIntervals	The value of vRtrOspfIfBadHelloIntervals is the total number of OSPF packets received where the hello interval given in packet was not equal to that configured on this interface since ospfAdminStat was last set to 'enabled'.
badLengths	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfBadLengths	The value of vRtrOspfIfBadLengths represents the total number of OSPF packets received on this interface with a total length not equal to the length given in the packet itself since ospfAdminStat was last set to 'enabled'.
badNeighbors	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfBadNeighbors	The total number of OSPF packets received where the neighbor information does not match the information this device has for the neighbor since ospfAdminStat was last set to 'enabled'.
badNetworks	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfBadNetworks	The total number of OSPF packets received with invalid network or mask since ospfAdminStat was last set to 'enabled'.

(7 of 12)

Statistic counter name	Source MIB	Description
badOptions	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfBadOptions	The value of vRtrOspfIfBadOptions is the total number of OSPF packets received with an option that does not match those configured for this interface or area since ospfAdminStat was last set to 'enabled'.
badPacketTypes	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfBadPacketTypes	The total number of OSPF packets received with an invalid OSPF packet type since ospfAdminStat was last set to 'enabled'.
badVersions	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfBadVersions	The total number of OSPF packets received with bad OSPF version numbers since ospfAdminStat was last set to 'enabled'.
badVirtualLinks	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfBadVirtualLinks	The total number of OSPF packets received on this interface that are destined to a virtual link that does not exist since ospfAdminStat was last set to 'enabled'.
discardPackets	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfDiscardPackets	The total number of OSPF packets discarded on this interface since ospfAdminStat was last set to 'enabled'.
retransmitOuts	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfRetransmitOuts	The total number of OSPF Retransmits sent on this interface since ospfAdminStat was last set to 'enabled'.
ospf.InterfaceTransmitStats		
databaseDescriptionPackets	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfTxDBDs	The total number of OSPF DataBase Description packets transmitted on this interface since ospfAdminStat was last set to 'enabled'.
helloPackets	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfTxHellos	The total number of OSPF Hello packets transmitted on this interface since ospfAdminStat was last set to 'enabled'.
linkStateAcknowledgements	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfTxLSAcks	The total number of OSPF Link State Acknowledgements transmitted on this interface since ospfAdminStat was last set to 'enabled'.
linkStateRequests	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfTxLSRs	The total number of OSPF Link State Requests (LSRs) transmitted on this interface since ospfAdminStat was last set to 'enabled'.
linkStateUpdates	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfTxLSUs	The total number of OSPF Link State Updates (LSUs) transmitted on this interface since ospfAdminStat was last set to 'enabled'.
totalPackets	TIMETRA-OSPF-MIB.vRtrOspfIfEntry.vRtrOspfIfTxPackets	The total number of OSPF packets transmitted on this interface since ospfAdminStat was last set to 'enabled'.
ospf.NeighborGeneralStats		
events	OSPF-MIB.ospfNbrEntry.ospfNbrEvents	The number of times this neighbor relationship has changed state, or an error has occurred.
retransmissionQueueLength	OSPF-MIB.ospfNbrEntry.ospfNbrLsRetransQLen	The current length of the retransmission queue.
ospf.NeighborStatusStats		
badMtus	TIMETRA-OSPF-MIB.vRtrOspfNbrEntry.vRtrOspfNbrBadMTUs	The value of vRtrOspfNbrBadMTUs is the total number of times when the MTU in a received database description packet was larger than the MTU of the receiving interface since ospfAdminStat was last set to 'enabled'.

(8 of 12)

Statistic counter name	Source MIB	Description
badNeighborStates	TIMETRA-OSPF-MIB.vRtrOspfNbrEntry.vRtrOspfNbrBadNbrStates	The value of vRtrOspfNbrBadNbrStates is the total number of OSPF packets received when the neighbor state was not expecting to receive this packet type since ospfAdminStat was last set to 'enabled'.
badPackets	TIMETRA-OSPF-MIB.vRtrOspfNbrEntry.vRtrOspfNbrBadPackets	The value of vRtrOspfNbrBadPackets is the total number of times when an LS update was received with an illegal LS type or an option mismatch since ospfAdminStat was last set to 'enabled'.
badSequenceNumbers	TIMETRA-OSPF-MIB.vRtrOspfNbrEntry.vRtrOspfNbrBadSeqNums	The value of vRtrOspfNbrBadSeqNums is the total number of times when a database description packet was received with a sequence number mismatch since ospfAdminStat was last set to 'enabled'.
deadTimeOutstanding	TIMETRA-OSPF-MIB.vRtrOspfNbrEntry.vRtrOspfNbrDeadTimeOutstanding	This value represents the amount of time in seconds until the dead-router interval expires. Normally, this value should not be significantly smaller than the configured dead router interval minus one hello interval.
duplicates	TIMETRA-OSPF-MIB.vRtrOspfNbrEntry.vRtrOspfNbrDuplicates	The value of vRtrOspfNbrDuplicates is the total number of times when a duplicate database description packet was received during the Exchange state since ospfAdminStat was last set to 'enabled'.
lastEventTime	TIMETRA-OSPF-MIB.vRtrOspfNbrEntry.vRtrOspfNbrLastEventTime	This time contains the value of sysUpTime when the last event occurred that affected the adjacency to the neighbour.
lsaInstallFailed	TIMETRA-OSPF-MIB.vRtrOspfNbrEntry.vRtrOspfNbrLsaInstallFailed	The value of vRtrOspfNbrLsaInstallFailed is the total number of times an LSA could not be installed into the LSDB due to a resource allocation issue since ospfAdminStat was last set to 'enabled'.
lsaNotInLSDB	TIMETRA-OSPF-MIB.vRtrOspfNbrEntry.vRtrOspfNbrLsaNotInLsdbs	The value of vRtrOspfNbrLsaNotInLsdbs is the total number of times when an LS request was received for an LSA not installed in the LSDB of this device since ospfAdminStat was last set to 'enabled'.
optionMismatches	TIMETRA-OSPF-MIB.vRtrOspfNbrEntry.vRtrOspfNbrOptionMismatches	The value of vRtrOspfNbrOptionMismatches is the total number of times when a LS update was received with an option mismatch since ospfAdminStat was last set to 'enabled'.
upTime	TIMETRA-OSPF-MIB.vRtrOspfNbrEntry.vRtrOspfNbrUpTime	This value represents the uninterrupted time, in hundredths of seconds, the adjacency to this neighbour has been up.
ospf.VirtualLinkGeneralStats		
events	OSPF-MIB.ospfVirtIfEntry.ospfVirtIfEvents	The number of state changes or error events on this Virtual Link
lsaCount	OSPF-MIB.ospfVirtIfEntry.ospfVirtIfLsaCount	The total number of link-local link state advertisements in this virtual interface's link-local link state database.
ospf.VirtualLinkReceiveStats		

(9 of 12)

Statistic counter name	Source MIB	Description
databaseDescriptionPackets	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfRxDBDs	The total number of OSPF DataBase Description packets received on this virtual interface.
helloPackets	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfRxHellos	The total number of OSPF Hello packets received on this virtual interface.
linkStateAcknowledgements	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfRxLSAcks	The total number of Link State Acknowledgements received on this virtual interface.
linkStateRequests	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfRxLSRs	The total number of OSPF Link State Requests (LSRs) received on this virtual interface.
linkStateUpdates	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfRxLSUs	The total number of OSPF Link State Updates (LSUs) received on this virtual interface.
totalPackets	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfRxPackets	The total number of OSPF packets received on this virtual interface since it was created.
ospf.VirtualLinkStatusStats		
authorizationFailures	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfAuthFailures	The total number of OSPF packets received on this virtual interface with invalid authentication keys.
badAreas	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfBadAreas	The total number of OSPF packets received on this virtual interface with area mismatches.
badAuthorizationTypes	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfBadAuthTypes	The total number of OSPF packets received on this virtual interface with invalid authentication types.
badDeadIntervals	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfBadDeadIntervals	The value of vRtrOspfVirtIfBadDeadIntervals is the total number of OSPF packets received where the dead interval given in the packet was not equal to that configured on this virtual interface since ospfAdminStat was last set to 'enabled'.
badDestinationAddresses	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfBadDstAdrs	The total number of OSPF packets received on this virtual interface with invalid destination IP address.
badHelloIntervals	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfBadHelloIntervals	The value of vRtrOspfVirtIfBadHelloIntervals is the total number of OSPF packets received where the hello interval given in packet was not equal to that configured on this virtual interface since ospfAdminStat was last set to 'enabled'.
badLengths	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfBadLengths	The value of vRtrOspfVirtIfBadLengths represents the total number of OSPF packets received on this virtual interface with a total length not equal to the length given in the packet itself since ospfAdminStat was last set to 'enabled'.
badNeighbors	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfBadNeighbors	The total number of OSPF packets received where the neighbor information does not match the configuration this device has for the neighbor.
badNetworks	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfBadNetworks	The total number of OSPF packets received on this virtual interface with invalid network or mask fields.

(10 of 12)

Statistic counter name	Source MIB	Description
badOptions	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfBadOptions	The value of vRtrOspfVirtIfBadOptions is the total number of OSPF packets received with an option that does not match those configured for this virtual interface or transit-area since ospfAdminStat was last set to 'enabled'.
badPacketTypes	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfBadPacketTypes	The total number of OSPF packets received on this virtual interface with invalid OSPF packet types.
badVersions	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfBadVersions	The total number of OSPF packets received on this virtual interface with invalid OSPF version numbers.
discardPackets	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfDiscardPackets	The total number of OSPF packets discarded on this virtual interface.
retransmitOuts	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfRetransmitOuts	The total number of OSPF packets retransmitted on this virtual interface.
ospf.VirtualLinkTransmitStats		
databaseDescriptionPackets	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfTxDBDs	The total number of OSPF DataBase Description packets transmitted on this virtual interface.
helloPackets	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfTxHellos	The total number of OSPF Hello packets transmitted on this virtual interface since it was created.
linkStateAcknowledgements	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfTxLSAcks	The total number of OSPF Link State Acknowledgements transmitted on this virtual interface.
linkStateRequests	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfTxLSRs	The total number of OSPF Link State Requests (LSRs) transmitted on this virtual interface.
linkStateUpdates	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfTxLSUs	The total number of OSPF Link State Updates (LSUs) transmitted on this virtual interface.
totalPackets	TIMETRA-OSPF-MIB.vRtrOspfVirtIfEntry.vRtrOspfVirtIfTxPackets	The total number of OSPF packets transmitted on this virtual interface since it was created.
ospf.VirtualNeighborGeneralStats		
events	OSPF-MIB.ospfVirtNbrEntry.ospfVirtNbrEvents	The number of times this virtual link has changed its state, or an error has occurred.
retransmissionQueueLength	OSPF-MIB.ospfVirtNbrEntry.ospfVirtNbrLsRetransQLen	The current length of the retransmission queue.
ospf.VirtualNeighborStatusStats		
badMtus	TIMETRA-OSPF-MIB.vRtrOspfVirtNbrEntry.vRtrOspfVirtNbrBadMTUs	The value of vRtrOspfVirtNbrBadMTUs is the total number of times when the MTU in a received database description packet was larger than the MTU of the receiving interface since ospfAdminStat was last set to 'enabled'.
badPackets	TIMETRA-OSPF-MIB.vRtrOspfVirtNbrEntry.vRtrOspfVirtNbrBadPackets	The value of vRtrOspfVirtNbrBadPackets is the total number of times when an LS update was received with an illegal LS type or an option mismatch since ospfAdminStat was last set to 'enabled'.

(11 of 12)

Statistic counter name	Source MIB	Description
badSequenceNumbers	TIMETRA-OSPF-MIB.vRtrOspfVirtNbrEntry.vRtrOspfVirtNbrBadSeqNums	The value of vRtrOspfVirtNbrBadSeqNums is the total number of times when a database description packet was received with a sequence number mismatch since ospfAdminStat was last set to 'enabled'.
badVirtualNeighborStates	TIMETRA-OSPF-MIB.vRtrOspfVirtNbrEntry.vRtrOspfVirtNbrBadNbrStates	The value of vRtrOspfVirtNbrBadNbrStates is the total number of OSPF packets received when the virtual neighbor state was not expecting to receive this packet type since ospfAdminStat was last set to 'enabled'.
deadTimeOutstanding	TIMETRA-OSPF-MIB.vRtrOspfVirtNbrEntry.vRtrOspfVirtNbrDeadTimeOutstanding	This value represents the amount of time in seconds until the dead-router interval expires. Normally, this value should not be significantly smaller than the configured dead router interval minus one hello interval.
duplicates	TIMETRA-OSPF-MIB.vRtrOspfVirtNbrEntry.vRtrOspfVirtNbrDuplicates	The value of vRtrOspfVirtNbrDuplicates is the total number of times when a duplicate database description packet was received during the Exchange state since ospfAdminStat was last set to 'enabled'.
lastEventTime	TIMETRA-OSPF-MIB.vRtrOspfVirtNbrEntry.vRtrOspfVirtNbrLastEventTime	This time signifies the value of sysUpTime when the last event occurred that affected the adjacency to the virtual neighbour.
lsaInstallFailed	TIMETRA-OSPF-MIB.vRtrOspfVirtNbrEntry.vRtrOspfVirtNbrLsaInstallFailed	The value of vRtrOspfVirtNbrLsaInstallFailed is the total number of times when an LSA could not be installed into the LSDB due to a resource allocation issue since ospfAdminStat was last set to 'enabled'.
lsaNotInLSDB	TIMETRA-OSPF-MIB.vRtrOspfVirtNbrEntry.vRtrOspfVirtNbrLsaNotInLsdbs	The value of vRtrOspfVirtNbrLsaNotInLsdbs is the total number of times when an LS request was received for an LSA not installed in the LSDB of this router since ospfAdminStat was last set to 'enabled'.
optionMismatches	TIMETRA-OSPF-MIB.vRtrOspfVirtNbrEntry.vRtrOspfVirtNbrOptionMismatches	The value of vRtrOspfVirtNbrOptionMismatches is the total number of times when a LS update was received with an option mismatch since ospfAdminStat was last set to 'enabled'.
upTime	TIMETRA-OSPF-MIB.vRtrOspfVirtNbrEntry.vRtrOspfVirtNbrUpTime	This value represents the uninterrupted time, in hundredths of seconds, the adjacency to this virtual neighbour has been up.

(12 of 12)

30.2 Workflow for statistics collection

- 1 Create a file policy to specify:
 - the frequency of accounting statistics log collection from the managed devices
 - the compact flash device where the accounting statistic logs are stored as the counters are collected and the completed logs are stored
 - how long the accounting collected statistics logs are stored
- 2 Create multiple accounting policies to determine how statistics are collected for each business model or type of service provided.

The statistics logs are retrieved and stored in the 5620 SAM database as specified in the file policies and accounting policies.

- 3 Modify existing accounting policies or create new policies as required.
- 4 Monitor performance statistics data from the GUI based on:
 - a Services based on applied accounting policies.
 - b Equipment and other network objects using near-real-time network performance statistics logged from the managed devices. Modify the network statistics counter collection policy for network ports as required.

30.3 Statistics menus

Table 30-3 lists the statistics menus and their functions.

Table 30-3 5620 SAM statistics menus

Menu option	Function
Policies→File Policy Manager	Create one or more file policies.
Policies→Accounting Policy Manager	Create one or more accounting policies to manage statistics collection.
Find→Browse Log Records	View statistics logs

30.4 Statistics procedure list

Table 30-4 lists the procedures for using statistics.

Table 30-4 5620 SAM statistics procedures list

Procedure	Purpose
To create or modify a file policy	Specify how often log files of collected statistics counters are collected and managed.
To create or modify an accounting policy	Specify the types of statistics collected on a per-usage and per-service basis.
To view equipment and other object-based performance statistics	Monitor near-real time statistics on network equipment and other network objects, such as protocols.
To modify equipment and object-based performance statistics policies	Set specific polling and log collection policies for statistics classes and counters, on a per object and per statistics class basis.
To view statistics logs	View statistic log files

30.5 Performance monitoring using statistics procedures

Use the following procedures to perform 5620 SAM statistics-related tasks.

Procedure 30-1 To create or modify a file policy

A file policy is used in tandem with an accounting policy to manage statistics collection. You can create multiple file policies.

- 1 Choose Policies→File Policy Manager from the 5620 SAM main menu.

The File Policy Manager search form appears.

- 2 You can:

- a Create a policy by clicking on the Create File Policy button.

The File Policy Global Policy (Create) form appears, as shown in Figure 30-2. Go to step 3.

Figure 30-2 File Policy form

ID	Description	Local	Log ID	Collection (min)
2	description-83	<input type="checkbox"/>	99	60
3	description-84	<input type="checkbox"/>	85	60
4	description-85	<input type="checkbox"/>	91	60
5	description-86	<input type="checkbox"/>	80	60
6	description-87	<input type="checkbox"/>	89	60
7	description-88	<input type="checkbox"/>	90	60
8	description-89	<input type="checkbox"/>	93	60
9	description-90	<input type="checkbox"/>	83	60
10	description-91	<input type="checkbox"/>	82	60

- b Modify an existing policy:

- i Use the filter form to narrow the search for an existing policy.
- ii Specify the Policy scope parameter to set a local or global policy search. Local policies are those policies applied to specific managed devices.
- iii Click on the Search button.
The list of file policies appears.
- iv Choose a file policy from the list.

- v Click on the Edit button.

The File Policy Global Policy (Edit) form appears.

- 3 From the General tab, determine the configuration action by setting the Configuration Action parameter.
 - overwrite an existing file policy if the configuration parameters are the same
 - merge the changes to the file policy with the current file policy being configured
 - fail the creation of the file policy if there is an existing policy
- 4 Enter a displayed name and description to distinguish the file policy.
- 5 Specify the Rollover (min) parameter to set the file rollover time of the accounting statistics files.



Note — The managed devices have sufficient resources to support large scale statistical policy usage. Ensure that all collection intervals, file retention intervals, and rollover intervals are sufficient. Also ensure that statistics are retrieved from the storage devices on a regular basis.

- 6 Specify the a Retention (hr) parameter to set the interval, in hours, to determine how long the accounting statistics log files are kept.

The retention interval is the minimum amount of time that the logs are stored on the storage media. Any files that have not been transferred by FTP from the storage media by the retention interval may be deleted, or the logs may remain longer if there is available space.

- 7 Specify the Drive parameter to indicate where the statistics are to be collected from. You can choose an application specific location or from a location specified on the managed device.

Choose the flash storage media appropriate for storage. You can specify different flash drives for different policies, depending on need and the size of the logging data to be stored.

- 8 Specify the Backup Drive parameter to indicate where the statistics are to be backed up. You can choose an application specific location or from a location specified on the managed device.

- 9 Click on:

- a The Local Definitions tab to view accounting file policies in effect on managed devices.
 - b The Logs tab button to view any logs created using the specified file policy.
 - c The Access L2 Interfaces or Access L3 Interfaces tab button to view any interfaces using the specified file policy.
 - d The Fault tab button to view any alarm raised against the file policy
-

Procedure 30-2 To create or modify an accounting policy

An accounting policy is used in tandem with a file policy to manage statistics collection. You can create multiple accounting policies.

- 1 Choose Policies→Accounting Policy Manager from the 5620 SAM main menu.
- 2 You can:
 - a Create a policy by clicking on the Create Accounting Policy button.

The Accounting Policy Manager (Create) form appears with the General tab button selected, as shown in Figure 30-3. Go to step 3.

Figure 30-3 Accounting Policy Manager (Create) form - General

- b Modify an existing policy:
 - i Filter to narrow the search for an existing policy.
 - ii Specify the policy scope using the Policy scope parameter. Local policies are those policies applied to specific managed devices.
 - iii Click on the Search button.
The list of accounting policies appears.
 - iv Choose an accounting policy from the list.
 - v Click on the Edit button.
The Accounting Policy Global Policy (Edit) form appears.

- 3 From the General tab, configure the parameters.
- 4 Determine the configuration action.
 - overwrite an existing accounting policy if the configuration parameters are the same
 - merge the changes to the accounting policy with the current file policy being configured
 - fail the creation of the accounting policy if there is an existing policy
- 5 Choose a displayed name and description to distinguish the accounting policy.
- 6 Specify the Type parameter to indicate the types of accounting statistics collected by the accounting policy. See Table 30-1 for more information. Network statistics are network interface statistics. Service statistics are related to service access points through which customer data flows in the ingress or egress direction.

You can create accounting policies for any combination of:

- service ingress octet
 - service egress octet
 - service ingress packet
 - service egress packet
 - network ingress octet
 - network egress octet
 - network ingress packet
 - network egress packet
 - compact service in octet
 - compact service in ingress
 - combined network in egress octet
 - combined service in egress octet
 - combined service in egress
- 7 Specify the Default parameter to true to collect the statistics for the accounting policy created.
 - 8 Specify the Collection Interval (m) parameter to indicate how often the accounting statistics counters for the selected Type parameter are logged.



Note — The managed devices have sufficient resources to support large scale statistical policy usage. Ensure that all collection intervals, file retention intervals, and rollover intervals are sufficient. Also ensure that statistics are retrieved from the storage devices on a regular basis.

- 9 Choose a file policy.
 - a Set the Name parameter to the name of an existing file policy.
 - b Click on the Select button and choose a file policy from the list.
Click on the OK button.

The file policy is shown in the Name parameter.
 - c Click on the Remove button to remove an existing file policy from the Name parameter.

Choose a new file policy.
- 10 Click on the OK button.

The Accounting Policy Manager form appears.

- 11** Click on the Search button without choosing a filter.

The new accounting policy appears in the list.

- 12** Click on an accounting policy in the list and click on the Edit button.

The Accounting Policy (Edit) form appears.

- 13** Click on:

- a** The General tab button to view administrative state information. You can change the administrative state of statistics collection for the object.

- Up to keep collecting statistics
- Down to stop collecting statistics
- Not Operational to indicate that the equipment or service is not in use

- b** The Access L2 Interfaces or Access L3 Interfaces tab button to view any interfaces using the specified file policy.

- c** The Fault tab button to view any alarm raised against the file policy.

- d** The Global Definition tab button to view any instances of the accounting policy being used locally on equipment or services.

- i** Click on a row representing the local instance.

- ii** Click on the Edit button.

The policy form for the specific equipment or service appears. The Global Definitions tab changes to a Local Definitions tab.

- iii** Click on the OK button to change the parameters, or click the Cancel button to close the form.

- 14** You can:

- a** Choose an accounting policy when you create a service. Alcatel recommends that you use this method for accounting policies.

- b** Click on the Distribute button to send the accounting policy to the network devices. Alcatel does not recommend that you use this method.

- c** Click on the Delete button to remove an accounting policy.

- d** Click on the Free Unused button to remove any accounting policies not being used by a service or other object.

- e** Click on the Copy button to create another accounting policy with the same parameter settings.
-

Procedure 30-3 To view equipment and other object-based performance statistics

Equipment and object-based performance statistics help operators monitor the usage of physical and logical network elements in near-real time. Statistics logs are used to show equipment and logical network object usage rates.

- 1 Open a view of the equipment or logical object.

For example, to view port statistics, click on the Network tab in the navigation tree and navigate to a port using the path Router→Shelf→Card Slot→Daughter Card Slot→Port. Right-click on the port icon and choose Properties from the contextual menu.

- 2 Choose the equipment on which to view statistics.

You can view statistics on logical or physical interfaces, for example, SONET ports.

- 3 Click on the Statistics tab button.

Additional statistics tabs appear. The tabs that appear are determined by the type of equipment. Click on the tab buttons to view specific statistics. Table 30-5 lists the general classes of statistics displayed. Table 30-2 provides a complete list.

Table 30-5 Performance statistics classes supported

Performance statistics class	Example
Ethernet	Broadcast packets, dropped events, fragments, and packets of specific octet size
SONET/SDH section, line, path, and traffic	Coding violations, errored and severely errored seconds
Physical	Interface statistics such as received, transmitted, and outbound packets; and Dot3 statistics

- 4 Review the most recent interval of performance statistics collected for the equipment or object.

By default, the rows are listed by most recent polling interval. You can sort based on the monitored object column, which represents the physical or logical object.

- 5 You can update the list of performance statistics using the Resync button.

- i Click on the appropriate statistics tab button.
- ii Click on the Resync button.
- iii Confirm the resynchronization by clicking on the Yes button.

The latest statistics are displayed.

- iv Repeat for each statistics tab, as required.

- 6 Click on the View History button.

- 7 Create a filter, or use the provided filter, and click on the OK button.

The performance statistics information appears in the Browse Log Records form as a series of rows, one for each interval.

- 8 Click on a row of statistics and click on the Edit button.

The statistics form appears. Figure 30-4 shows a sample statistics form.

Figure 30-4 Statistics form

The screenshot shows a window titled "Fast Ether Port - Port 1/1/2, Chassis - 1, 10.1.1.30 [Edit]". The "Statistics" tab is selected. The form displays the following data:

Time Captured:	11/05/2003 08:27:21 877 EST	Periodic Time:	0 days 01:
Monitored Object:	network:10.1.1.30:chassis-1:slot-01:card:mdaSlot-1:mda:port-002		
Received Broadcast Packets:	0	Received Broadcast Packets Periodic:	0
Received Multicast Packets:	0	Received Multicast Packets Periodic:	0
Received Total Octets:	0	Received Total Octets Periodic:	0
Received Unicast Packets:	100834	Received Unicast Packets Periodic:	6696
Transmitted Broadcast Packets:	0	Transmitted Broadcast Packets Periodic:	0
Transmitted Multicast Packets:	95011	Transmitted Multicast Packets Periodic:	6311
Transmitted Total Octets:	0	Transmitted Total Octets Periodic:	0
Transmitted Unicast Packets:	95011	Transmitted Unicast Packets Periodic:	6311

Buttons at the bottom: Resync, Edit Policy..., View History...

- 9 Review the statistics data, as required.

Procedure 30-4 To modify equipment and object-based performance statistics policies

The collection of statistics for equipment and other logical network objects is independent per statistics class. Therefore you can fine-tune the collection and polling policies per object type.



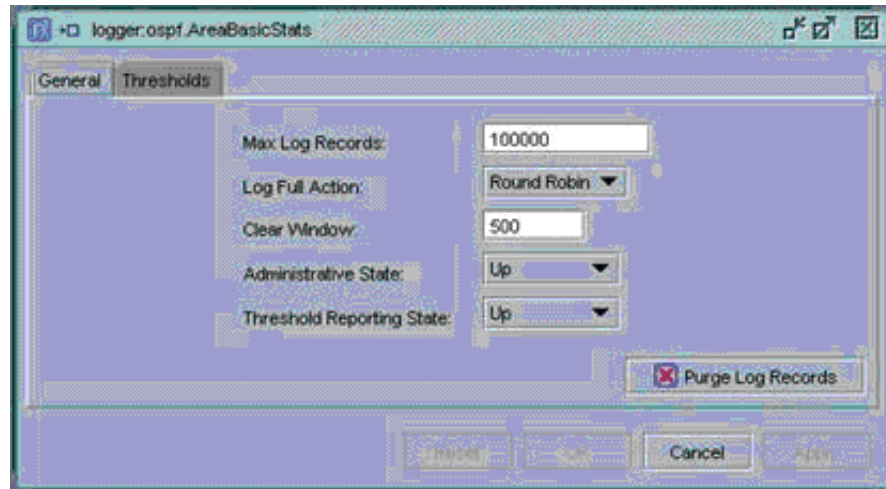
Note — When you change polling policies for one statistics class for one network object, the same changes apply to all other network objects that use the same statistics class.

- 1 Perform Procedure 30-3 until step 3.
- 2 Click on the Edit Policy button to open the statistics polling policy configuration form for the specific equipment or object.

The polling policy configuration form (called the logger form on the GUI) appears.

- 3 Click on the General tab button. The General tab contains parameters that determine the polling configuration. The statistics class full name appears in the titlebar of the configuration form as shown in Figure 30-5. For example, logger.ospf.AreaBasicStats is the statistics class.

Figure 30-5 Polling policy configuration form - General



- Set the Max Log Records parameter to specify the maximum number of statistics records supported for this statistics class.
 - Set the Log Full Action parameter to specify how statistics are handled when the log file is full. You can stop collection, or round-robin collection to drop the oldest records and keep the latest records.
 - Set the Clear Window parameter to specify the number of log records that are removed when the round-robin log full action takes effect. This removes the specified number of log records to accommodate new log records.
 - Specify whether the Administrative State parameter is up or down. You must set the Administrative State parameter to Up to collect statistics for the statistics class.
 - Set the Threshold Reporting State to Up to report threshold crossing alarms.
- 4 Click on the Thresholds tab button, if you set the Threshold Reporting State to Up in step 3. The Thresholds tab button contains parameters that specify thresholds for each counter in the statistics class.

Specify a number for the periodic threshold. If that threshold is exceeded for that statistics counter, the user notified by a threshold crossing alarm, as shown in Figure 30-6.

Figure 30-6 Polling policy configuration form - Threshold

- 5 Click on the Apply button to save the changes. Click on the OK button to close the form.

Procedure 30-5 To view statistics logs

Statistics logs contain the statistics data for network ports that collect performance statistics.

- 1 Choose Find→Browse Log Records from the 5620 SAM main menu.
The Filter (Browse Log Records) form appears.
- 2 Modify the filter to generate a list of statistical data.
 - a Specify the Log Class parameter by choosing a type of statistic from a drop-down list of log classes. The log classes indicate which classes of statistics are available.
 - Access Interface Stp Stats
 - Area Basic Stats
 - Area Interface Stats
 - Area Lsa Stats
 - Dot 3 stats
 - Dynamic Lsp Stats
 - Ethernet Stats
 - Interface Stats
 - Tunnel Stats
 - Virtual Neighbor Stats
 - Virtual Link Stats
 - LSP Stats
 - Media Independence Stats
 - Mpls Stats
 - Neighbor Stats
 - Peer Stats
 - Ppp Stats
 - Route Stats
 - Rsvp Stats
 - Site Stats
 - SONET Stats
 - Virtual Neighbor Stats
 - b Specify the Log Type parameter. Choose from a drop-down list of the types of log records, for example the most current set of data for the statistics class, or data that has already been logged.

- c Choose a filter from the Unused Properties list. Available filters are determined by the log class selected. For each log class, there are multiple individual statistics on which you can filter.

For example, if you choose OSPF-related Area Basic statistics as the log class, specific counters for that class, such as Area Border Router Count and Maintained Object, appear in the Unused Properties list. These counters are available when you view the statistic log.

- 3 Click on the OK button.

The Browse Log Records form appears, as shown in Figure 30-7.

Figure 30-7 Browse Log Records form

Time Captured	Monitored Object	Received Multic...	Receiv...
01/07/2004 09:09:31 234 EST	network:10.1.1.23.chas...	0	0
01/13/2004 09:20:59 415 EST	network:10.1.1.23.chas...	0	0
01/13/2004 09:21:08 308 EST	network:10.1.1.23.chas...	0	0
01/14/2004 15:00:52 063 EST	network:10.1.1.23.chas...	0	0
01/15/2004 13:49:49 379 EST	network:10.1.1.31.chas...	0	0
01/15/2004 13:49:49 387 EST	network:10.1.1.31.chas...	650569	11988
01/15/2004 13:49:52 958 EST	network:10.1.1.23.chas...	0	0
01/15/2004 13:49:52 967 EST	network:10.1.1.23.chas...	0	0
01/15/2004 13:49:52 982 EST	network:10.1.1.23.chas...	1308056	11992
01/15/2004 13:49:53 823 EST	network:10.1.1.30.chas...	0	0
01/15/2004 13:49:53 829 EST	network:10.1.1.30.chas...	0	0
01/15/2004 13:49:53 834 EST	network:10.1.1.30.chas...	5258	922337
12/05/2003 14:09:23 132 EST	network:10.1.1.23.chas...	0	0
12/05/2003 14:09:23 302 EST	network:10.1.1.23.chas...	0	0
12/05/2003 14:09:23 351 EST	network:10.1.1.23.chas...	0	0
12/05/2003 14:09:23 399 EST	network:10.1.1.23.chas...	0	0
12/05/2003 14:09:23 446 EST	network:10.1.1.23.chas...	0	0
12/05/2003 14:09:23 616 EST	network:10.1.1.23.chas...	0	0
12/05/2003 14:09:23 667 EST	network:10.1.1.23.chas...	0	0
12/05/2003 14:09:23 732 EST	network:10.1.1.23.chas...	0	0
12/05/2003 14:09:23 780 EST	network:10.1.1.23.chas...	0	0
12/05/2003 14:09:23 845 EST	network:10.1.1.23.chas...	0	0
12/05/2003 14:09:24 075 EST	network:10.1.1.23.chas...	0	0

- 4 Scroll the listed logs to view the statistics. By default, the rows are sorted to show the most recently collected logs first. Each row represents a network object.
 - a Scroll across the row of each log to view the statistics for the equipment or object. Table 30-6 describes the additional logged statistic information. Table 30-2 lists all the performance statistics classes available.

Table 30-6 Additional statistics log information

Parameter	Description
Time Captured	Time log file was created
Periodic Time	Time period in which statistics were collected

(1 of 2)

Parameter	Description
Monitored Object	Name of the object for which the logged statistics were collected
<i>Names of statistics</i>	Each column is a statistic counter collected in the polling period configured for that statistics class. For example, Figure 30-7 shows the first column of statistics counter as Received Multicast Packets for each of the statistical intervals. See Table 30-2 for a complete list of counters.

(2 of 2)

- b** Double-click on a row of the log.

The form of logged statistics for the network object appears. See Table 30-6 for the logged statistical information. Figure 30-8 shows a sample log record.

Figure 30-8 Sample log record

The screenshot shows a window titled "logger:phys.InterfaceAdditionalStats\network_10.1.1.30_chassis-1_slot-11_card_port-001". It contains a form with the following fields:

- Time Captured: 01/15/2004 13:49:53 834 EST
- Periodic Time: 0 days 00:40:11 198
- Monitored Object: network:10.1.1.30:chassis-1:slot-11:card:port-001
- Received Broadcast Packets: 0
- Received Broadcast Packets Periodic: 0
- Received Multicast Packets: 5258
- Received Multicast Packets Periodic: 3372036847422262
- Received Total Octets: 675768
- Received Total Octets Periodic: 3372035974852026
- Received Unicast Packets: 6059
- Received Unicast Packets Periodic: 3372036846202108
- Transmitted Broadcast Packets: 0
- Transmitted Broadcast Packets Periodic: 0
- Transmitted Multicast Packets: 854
- Transmitted Multicast Packets Periodic: 3372036853404007
- Transmitted Total Octets: 296440
- Transmitted Total Octets Periodic: 3372036368246162
- Transmitted Unicast Packets: 854
- Transmitted Unicast Packets Periodic: 3372036853404007

At the bottom of the window, there are buttons for "Resync", "Edit Policy...", "View History...", and "Close".

- 5** Click on the Resync button to generate the latest set of logged statistics.

Glossary

Numerics

5620 SAM	Alcatel 5620 Service Aware Manager The 5620 SAM is the network manager portfolio of modules for the 7750 SR and 7450 ESS.
5620 SAM client	The 5620 SAM client provides a GUI to configure IP network elements.
5620 SAM database	The 5620 SAM database stores network objects and configurations.
5620 SAM server	The 5620 SAM server mediates between the 5620 SAM database, 5620 SAM client, and the network.
5620 SAM-A	Alcatel 5620 SAM Assurance The 5620 SAM-A provides service assurance functionality.
5620 SAM-E	5620 SAM Element Manager The 5620 SAM-E provides network element configuration and management functionality.
5620 SAM-O	Alcatel 5620 SAM Open Interfaces The 5620 SAM-O provides an XML interface for OSS applications to interact with the 5620 SAM.
5620 SAM-P	Alcatel 5620 SAM Provisioning The 5620 SAM-P provides service provisioning functionality.
7450 ESS	7450 Ethernet Service Switch

7750 SR	<p>7750 Service Router</p> <p>The 7750 SR is a router that provides scalable, high-speed private data services with SLAs.</p>
A	
AAA	<p>Authentication, authorization, and accounting</p> <p>The functions of security-based protocols, such as RADIUS, to ensure secure communications.</p>
ACL	<p>access control list</p> <p>An access control list, which is also known as a filter policy, is a template applied to services or ports to control network traffic into (ingress) or out (egress) of an SAP or port based on IP and MAC matching criteria. Filters are applied to services to examine packets entering or leaving a SAP or network interface. An ACL policy can be used on several interfaces. The same filter can be applied to ingress traffic, egress traffic, or both.</p>
adjacency	<p>An adjacency is the portion of the local routing information that pertains to the reachability of a single neighbor end system or intermediate system. A separate adjacency is created for each neighbor, and for each level of routing on a broadcast circuit.</p>
alarm	<p>An alarm is a node-generated message created as a result of an event, such as an interface status change.</p>
API	<p>application programming interface</p> <p>An API is a set of programming functions and routines that provides an interface to the network for application programs. APIs translate high-level program code into low-level computer instructions that run the network. Thus, application programs (for example, word processors) can communicate with low-level programs handling network data traffic.</p>
area	<p>In the OSPF protocol, network management and scalability can be simplified by partitioning a network into regions. These OSPF network regions are called areas. Each area, also called a routing sub-domain, maintains detailed routing information about its own internal composition, and also maintains routing information which allows it to reach other areas.</p>
ARP	<p>Address Resolution Protocol</p> <p>ARP is a TCP/IP protocol used to convert an IP address into a physical address, such as an Ethernet address.</p>
AS	<p>autonomous system</p> <p>An AS is a collection of devices under one administrative entity that cooperates by using a common IGP (such as OSPF). AS is synonymous with the ISO term "routing domain". Routing between autonomous systems is done with an inter-AS or interdomain EGP, such as BGP-4.</p>
ASBR	<p>autonomous system boundary router</p>

In OSPF, an ASBR is a router that exchanges information with devices from other ASs. ASBRs are also used to import routing information about RIP, direct, or static routes from non-OSPF attached interfaces.

ATM asynchronous transfer mode

A transport and switching mechanism that employs 53-byte cells as a basic unit of transfer. Information is routed through the network in the cell using addressing information contained in the header.

B

BGP border gateway protocol

BGP is an IETF standard EGP used to propagate routing information between autonomous systems.

bridge Bridges connect two or more network segments which increases the network diameter. Bridges also help regulate traffic. They can send and receive transmissions but a bridge does not originate any traffic of its own other than a special Ethernet frame that allows it to communicate with other bridges.

C

CBS committed burst size

CBS specifies the amount of buffers that can be drawn from the reserved buffer portion of the queue's buffer pool. Once the reserved buffers for a given queue have been used, the queue contends with other queues for additional buffer resources up to the maximum burst size.

The CBS is provisioned on ingress and egress service queues within the service ingress QoS policies and service egress QoS policies, respectively. The CBS for a queue is specified in Kbytes.

The CBS for network queues are defined with the network buffer policies based on the forwarding class. The CBS for the queues for the forwarding class are defined as a percentage of buffer space for the buffer pool.

CE customer edge

A device with the functionality needed on the customer premises to access provider-provisioned services.

class of service *See* CoS

CLI command line interface

CLI is a command-driven, text-based user interface to manage a device.

CIR committed information rate

The CIR is the guaranteed minimum rate of throughput between two end-user devices over a network under normal operating circumstances. This rate, measured in bits or kb/s, is used in congestion control procedures.

circuit A circuit is a communications connection between two points. It has a line interface from which it transmits and receives data and signaling. A circuit is also known as a port, channel, or timeslot. An electronic circuit is one or more electronic components connected together to perform a specific function.

CLI command line interface

The CLI is an interface that allows the user to interact with the operating system by typing alphanumeric commands and optional parameters at a command prompt. UNIX and DOS provide CLIs.

confederation In BGP, a confederation is an AS that has been subdivided into smaller ASs called CMASSs. A confederation appears to be a single AS to other ASs and is recognized only by other confederation members.

CoS class of service

CoS is the degree of importance assigned to traffic. There are standard and premium classes of services. During queuing and forwarding, service points give preferential treatment to traffic that originates on elements configured for premium CoS.

CPE customer premises equipment

Network equipment that resides on the customer's premises.

CPM central processor module

The dual CPU control plane module is dedicated for system control, centralized protocol processing, and management.

CSNP complete sequence number PDU

CSV comma separated value

CSV is a way of recording parameters and values in text format, with each value followed by a comma.

D

device A generic term for a network element such as a router, switch, or bridge.

DSCP differentiated services codepoint

The DSCP is a six-bit field in the IP header that provides CoS on a per-packet basis.

DP drop precedence

Attribute of a packet which affects the probability of the packet being dropped within a CoS.

DSCP	<p>differentiated services code point</p> <p>A six-bit value encoded in the type of service field of an IP packet header, which identifies CoS and the DP the packet receives.</p>
DU	<p>downstream solicited</p> <p>An MPLS LDP technique, where LSRs distribute bindings to LSRs that have not explicitly requested them.</p>
E	
e-BGP	<p>extended border gateway protocol</p>
ECMP	<p>equal-cost multipath</p>
E-LSP	<p>EXP inferred LSP</p>
encapsulation	<p>Encapsulation is the addition of information to the beginning and end of data. Encapsulation is used by layered network protocols as data moves from one stack down to the next. Header and trailer information is added to the data at each layer. Encapsulation is also used to bridge connections between different types of networks.</p>
EXP	<p>EXPerminatal</p> <p>A field in the MPLS packet header.</p>
F	
fault	<p>A fault is a failure or defect in a network, causing the network, or part of the network, to malfunction.</p>
FCAPS	<p>Fault, Configuration, Administration, Performance, and Security</p> <p>The major functional areas for network and element configuration and management.</p>
FEC	<p>forwarding equivalency class</p> <p>A group of IP packets which are forwarded in the same manner, for example, over the same path, with the same forwarding treatment.</p>
FIB	<p>forwarding information base</p> <p>FIB is the set of information that represents the best forwarding information—for example, next IP hop—for each destination (or set thereof). The entries in the FIB are derived from the reachability information held in the RIB, subject to administrative routing.</p>
forwarding class	<p>A forwarding class, also called a CoS, provides to network elements a method to weigh the relative importance of one packet over another in a different forwarding class. Each forwarding class is important only in relation to other forwarding classes.</p>

Queues are created for a specific forwarding class to determine the manner in which the queue output is scheduled into the switch fabric and the type of parameters the queue accepts. The forwarding class of the packet, along with the in-profile or out-of-profile state, determines how the packet is queued and handled (the per-hop behavior at each hop along its path to a destination egress point).

FTP file transfer protocol

FTP is the Internet standard client-server protocol for transferring files from one computer to another. FTP generally runs over TCP or UDP.

G

GUI graphical user interface

A GUI is a computer user interface that incorporates graphics to make software easier to use.

GRE generic routing encapsulation

H

HQoS hierarchical quality of service

HQoS provides the ability to rate limit across multiple queues from either single or multiple access interfaces for a given customers.

HVPLS hierarchical virtual private LAN service

I

IBGP Interior Gateway Border Protocol

ICMP Internet Control Message Protocol

ICMP is a protocol that sends and receives the control and error messages used to manage the behavior of the TCP/IP stack. ICMP is defined in RFC 792.

IES Internet Enhanced Service

IES is a routed connectivity service where the subscriber communicates with an IP router interface to send and receive Internet traffic. An IES has one or more logical IP router interfaces, each with a SAP which acts as the access point to the subscriber network. IES allows customer-facing IP interfaces to participate in the same routing instance used for service network core routing connectivity. IES services require that the IP addressing scheme used by the subscriber be unique between other provider addressing schemes and possibly the entire Internet.

While the IES is part of the routing domain, the usable IP address space may be limited. This allows a portion of the service provider address space to be reserved for service IP provisioning, and be administered by a separate but subordinate address authority.

IP interfaces defined within the context of an IES service must have a SAP associated as the access point to the subscriber network. Multiple IES services are created to segregate subscriber-owned IP interfaces.

IETF internet engineering task force

The IETF is the organization that provides coordination of standards and specifications developed for IP network and related protocols.

IGP Interior Gateway Protocol

Generic term applied to any protocol used to propagate network reach and routing information within autonomous system.

I/O input/output

Connections between a system and its controlled devices (output) and incoming statuses (input).

IP internet protocol

IP is the network layer for the TCP/IP protocol suite. It is a connectionless, best-effort packet-switching protocol defined by the IETF.

IS intermediate system

This term is used interchangeably with router.

ISIS intermediate system to intermediate system

ISIS is an ISO standard link-state routing protocol. Integrated ISIS is an extension that allows ISIS to be used for route determination in IP networks.

J

JMS Java Message Service

JMS is an API that combines Java technology with enterprise messaging. The JMS API defines a common set of interfaces for creating applications for reliable asynchronous communication among components in a distributed computing environment, so that the applications are portable across different enterprise systems.

L

L3 Layer 3

LACP link aggregation control protocol

LACP is used to detect whether all local members of a LAG are physically connected to the remote ports that are part of the far end of the LAG.

LAG link aggregation group

A LAG increases the bandwidth available between two nodes by grouping up to eight ports into one logical link. The aggregation of multiple physical links allows for load sharing and offers seamless redundancy. If one of the links fails, traffic is redistributed over the remaining links. Up to eight links can be supported in a single LAG, and up to 64 LAGs can be configured on a node.

LAN local area network

A LAN is a group of computers or associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area, for example, within an office building.

LDP label distribution protocol

LDP is a signaling protocol used for MPLS path setup and teardown. An LDP is used by LSRs to indicate to other LSRs of the meaning of labels used to forward traffic.

LDP is defined in RFC 3036.

level 1 and level 2 intermediate system

These systems deliver and receive NPDU from other systems, and relay NPDU from other source systems to other destination systems. Level 1 systems route directly to systems within their own area, and route towards a level 2 system. A level 2 systems route towards another destination area or another routing area. Level 2 systems constitute the IS-IS backbone area.

LLC logical link control

LLC is the upper sublayer of the ISO model data link layer. LLC governs packet transmission as specified by IEEE 802.2.

L-LSP label only inferred LSP

load balancing Load balancing is the distribution of network traffic among the ports by a device so that no single port is overwhelmed, and network bandwidth is optimized.

LPE logical provider edge

A set of devices in a provider network that implement the functionality of a service, such as VPLS.

LSA link state advertisement

LSA describes the local state of a device or network, including the state of the device's interfaces and adjacencies. Each LSA is flooded throughout the routing domain. The collected LSAs of all devices and networks form the protocol's topological database.

LSP label switched path

LSPs support MPLS functionality and allow network operators to perform traffic engineering. There are two types of LSPs:

- **static LSP**
A static LSP specifies a static path. All devices that the LSP traverses must be configured manually with labels. No signaling is required.
- **signaled LSP**
A signaled LSP is an LSP that is set up using a signaling protocol. The signaling protocol allows labels to be assigned from an ingress router to an egress router. Signaling is triggered by the ingress router. Only the ingress router, and not the intermediate routers, must be configured. Signaling also facilitates path selection.

LSP classifier A method of filtering IP traffic flows on to an LSP.

LSP path A LSP associated with an MPLS path.

This could be an actual route, or a configured route. A configured route can be primary, secondary, or standby. An LSP could have at most one actual route, one primary route, and multiple standby or secondary routes.

LSR label switched router

An LSR is an MPLS node that runs MPLS control protocols and is capable of forwarding packets based on labels. An MPLS node may also be capable of forwarding native layer 3 packets.

M

MAC media access control

MAC is a sublayer of the data link layer, defined in IEEE 802.2 specifications, that is responsible for accessing the LAN medium. The MAC layer handles the recognition and identification of individual network devices.

Every computer and network node has a MAC address that is hardware-encoded.

MAF management access filter

MD5 message digest 5

MD5 is a security algorithm that takes an input message of arbitrary length and produces as an output a 128-bit message digest of the input. MD5 is intended for digital signature applications, where a large file must be compressed securely before being encrypted.

MDA media dependent adaptor

MDA is a pluggable interface module that distributes traffic between the network and the system I/O module. Also referred to as a daughter card.

MED multi-exit discriminator

menu bar	The menu bar is a tool on the GUI that organizes tasks across broad headings. You can perform functions on the application by selecting an action from the menu bar.
MIB	management information base
MP-BGP	multiprotocol border gateway protocol
MPLS	multiprotocol label switching MPLS is a technology in which forwarding decisions are based on fixed-length labels inserted between the data link layer and network layer headers to increase forwarding performance and flexibility in path selection.
MTU	Maximum transmission unit MTU is the largest unit of data that can be transmitted over a particular interface type in one packet. The MTU can change over a network.
N	
navigation tree	The navigation tree displays a view of all managed equipment, services, and protocols, and allows you to navigate through these components.
NE	network element A physical device in the network, such as a 7750 SR router, or a switch, such as the 7670 RSP.
neighbor	An adjacent system reachable by traversing a single sub-network by a PDU
network topology	A network topology is the layout of a network, which can include the way in which elements in a network, such as nodes, are connected and how they communicate.
networkstation	A UNIX platform where the 5620 SAM software runs.
NPDU	network protocol data unit
N-PE	network-facing provider edge A device that implements the control and signaling functions of a LPE.
NSSA	not-so-stubby-area NSSA is an OSPF area type where OSPF propagates any external routes that it obtains from the AS.
NTP	Network Time Protocol Internet protocol used to synchronise time between network equipment.
O	
OAM	operations, administration, and maintenance

A general term used to describe the costs, tasks involved, or other aspects of operating, administering, and managing a telecommunications network. The 5620 SAM provides a series of OAM tools to monitor and administer the network.

OC-N

Optical Carrier - level *N*

An optical SONET signal carried at the speed of *N*, for example OC-12 is a signal at 622.08 Mb/s.

OSPF

Open Shortest Path First

OSPF is an IETF standard link-state routing protocol used to determine the most direct path for a transmission in IP networks.

OSS

operational support system

A network management system supporting a specific management function, such as alarm surveillance and provisioning, in a service provider network.

P**PC**

personal computer

PDU

protocol data unit

A PDU is a message of a given protocol comprising payload and protocol-specific control information, typically contained in a header. PDUs pass over the protocol interfaces which exist between the layers of protocols, as indicated in the OSI model.

PE

provider edge

PHB

per-hop behavior

An IETF standard term for CoS plus DP.

PHP

penultimate hop popping

PIR

Peak Information Rate

The PIR is the peak data transfer rate for a path, such as a frame relay, VPC, VCC, or DE Service path. The PIR is the PCR converted to kb/s.

POS

packet over SONET

Q**QoS**

Quality of Service

QoS is a term for the set of parameters and their values that determine the performance of a virtual circuit. This service level is usually described in a network by delay, bandwidth, and jitter.

R

RADIUS	A remote user authentication, authorization, and accounting protocol.
RD	route distinguisher
RED	random early detection RED is a gateway that detects and avoids traffic congestion in a packet-switched network. Incoming congestion is detected by calculating the average queue size. If the gateway decides that the average queue size exceeds a predetermined threshold, it either randomly drops packets arriving at the gateway or sets a bit in the packet headers. The packet transmission rate is reduced until all the packets reach their destination.
RIP	Routing Information Protocol RIP is a Bellman-Ford routing protocol based on distance vector algorithms that measure the shortest path between two points on a network in terms of the number of hops between those points. Various forms of RIP are used to distribute routing information in IP, XNS, IPX, and VINES networks. <i>See also</i> OSPF.
router	A router is an interface device that connects two networks. It maintains configuration tables and uses various network protocols to select cost-effective routes that move data between a source and destination device. Also called a device.
routing instance	A routing instance is the configuration of a router, including information such as protocols, interfaces, routing, and policies.
routing protocol	A routing protocol is used to determine the correct route for packets within IP and IP/MPLS networks.
RSVP	Resource Reservation Protocol is used two ways: <ol style="list-style-type: none">1 RSVP is the process of reserving network and host resources to achieve a QoS for an application.2 RSVP is an IP-based protocol that is used for communicating application QoS requirements to intermediate transit nodes in a network. RSVP uses a soft-state mechanism to maintain path and reservation state in each node in the reservation path.
RT	route target
S	
SAP	service access point An SAP is a point of communication exchange between an application and the LLC or between layers of software.
SDP	service distribution path

	<p>A service distribution path acts as a logical way of directing traffic from one 7750 SR to another 7750 SR through a unidirectional service tunnel. The SDP terminates at the far-end 7750 SR, which directs packets to the correct service egress SAPs on that device. A distributed service consists of a configuration with at least one SAP on a local node, one SAP on a remote node, and an SDP binding the service to the service tunnel.</p>
service-level agreement	<p>See SLA.</p>
service tunnel	<p>A service tunnel is used by a service distribution path to unidirectionally direct traffic from one 7750 SR router to another. The service tunnel is provisioned with an encapsulation and the services are mapped to the service tunnel that most appropriately supports the service needs.</p>
SLA	<p>service-level agreement</p> <p>An SLA is a service contract between a network service provider and a subscriber that guarantees a particular QoS. SLAs are used for providing network availability and data-delivery reliability.</p>
SNMP	<p>Simple Network Management Protocol</p> <p>A protocol used for the transport of network management information between a network manager and a network element. SNMP is the most commonly used standard for most interworking devices.</p>
SNMP trap	<p>An SNMP trap is an unsolicited notification that indicates that the SNMP agent on the node has detected a node event, and that the network management domain should be aware of the event. SNMP trap information typically includes alarm and status information, and standard SNMP messages.</p>
SNMP trap log ID	<p>SNMP trap log ID is the ID of a log. A valid log ID must exist for alarms and traps to be sent to the trap receiver.</p>
Solaris	<p>The name for the UNIX operating system variant developed by SUN Microsystems.</p>
SONET	<p>Synchronous Optical Network</p> <p>SONET is an ANSI standard for fiber optic transmission of high-speed digital traffic. SONET allows internetworking of transmission products from multiple vendors and defines a physical interface, optical line rates known as OC signals, frame format, and an OAM protocol. The base rate is 51.84 Mb/s (OC-1), and higher rates are multiples of the base rate.</p> <p>SONET uses synchronous high-speed signals and provides easy access to low-speed signals by mapping them into VTs.</p> <p>SONET is a North American standard that is technically consistent with SDH, which is international.</p>
SPF	<p>shortest path first</p> <p>SPF is an algorithm used by IS-IS and OSPF to make routing decisions based on the state of network links.</p>

SSH	secure shell The SSH protocol is used to protect communications between two hosts by encrypting a Telnet or FTP connection between the 5620 SAM and some nodes. 5620 SAM uses SSH version 1.5. Both ends of the client/server connection are authenticated, and passwords are protected by being encrypted.
statistics	Statistics are the quantitative data collected in the 5620 SAM, which includes equipment statistics and network alarm statistics.
STM-N	Synchronous Transport Module - level <i>N</i> An SDH signal carried at the speed of <i>N</i> , for example STM-4 is a signal at 622.08 Mb/s.
STP	Spanning Tree Protocol The STP is specified in IEEE802.1d. This protocol automatically ensures a loop-free topology in any interconnection of Ethernet LAN or WAN devices.
subscriber	A subscriber is a customer who buys services from a network provider.
switch	Switches are Layer 2 devices that make it possible for several users to send information over a network at the same time without slowing each other down. Switches allow different nodes of a network to communicate directly with one another in an efficient manner.
T	
TACACS+	A remote user authentication, authorization, and accounting protocol.
TCP	transmission control protocol TCP is a protocol used, along with the Internet Protocol (IP), to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.
Telnet	Telnet is the Internet-standard TCP/IP protocol for remote terminal connection service. It allows a user at one site to interact with a remote timesharing system at another site as if the user's terminal connected directly to the remote machine. The Telnet command and program are used to log in from one Internet site to another. It gets the user to the login prompt of another host.
tiered architecture	Tiered architecture refers to the way in which the GUI and the network management components use a Java-based technology that provides distributed, secure, and scalable applications. This tiered architecture allows for scaling and fair load balancing, which improves performance.
T-LDP	targeted LDP

	An LDP session between indirect connect peers.
TTL	time to live
	An IETF specification that calls for a minimum default value of 64 hops before a data packet expires.
U	
UDP	user datagram protocol
UNIX	UNIX is a multi-user, multitasking operating system, which is used on mainframes, workstations, and PCs. UNIX is the basis of Solaris and SunOS, which are operating systems used by Sun workstations.
UI	user interface
	<i>See</i> GUI
V	
VC	virtual connection
	A technique ensuring that packets are delivered to the correct recipient in the same order as they were submitted.
virtual link	Virtual links connect separate elements of a backbone, and function as if they are unnumbered point-to-point networks between two devices. A virtual link uses the intra-area routing of its transit area (the non-backbone area that both devices share) to forward packets.
VLAN	virtual LAN
	A logical grouping of two or more nodes which are not necessarily on the same physical network segment but which share the same IP network number.
VLL	virtual leased line
	A virtual leased line is a type of VPN where IP is transported in a point-to-point manner. CPE devices are connected through nodes, and the nodes are connected to an IP tunnel.
VPLS	virtual private LAN service
	A VPLS is a type of VPN in which a number of sites are connected in a single bridged domain over an IP/MPLS network. Although the services may be from different locations, in a VPLS, they appear to be on the same LAN.
	When implemented with layer 2 interfaces, this service is called VPLS. When implemented with layer 3 interfaces, this service is called an IP-VPN
VPN	virtual private routed network

VPRN	virtual private network A network exhibiting at least some of the characteristics of a private network, even though it uses the resources of a public switched network.
VRF	virtual routing and forwarding A logical or virtual routing function with associated routing table that can be instantiated in a device capable of supporting IP VPN services.
W	
window	Windows are forms, panels of information, equipment drawings, or graphics that appear on a screen. Windows commonly allow a user to input data and initiate functions but some windows simply display information.
workflow	The 5620 SAM workflow is a defined series of tasks that describe how to install, configure, create, and manage services.
working pane	The working pane is a component of the 5620 SAM GUI that can include windows, drawings, and configuration forms.
WRED	weighted random early detection WRED is a variation of RED, but instead of dropping packets randomly when there is high traffic congestion, the packets are dropped based on traffic priority.
X	
X.733	ITU-T X.733 X.733 is the standard that describes the alarm reporting function.
XML	extensible markup language XML defines the syntax to customize markup languages. The markup languages are used to create, manage, and transmit documents across the Web.

Index

Numbers

- 5620 SAM, 2-2
 - changing configurations, 2-2
 - CLI, 12-2
 - managing 7750 SR security, 9-2
 - new features, 2-4
- 5620 SAM GUI; *See* GUI
- 5620 SAM workflow, 1-2
 - configuring end-user services, 1-2
 - installing software, 1-2
 - managing end-user services, 1-2
- 7450 ESS
 - device support, 13-6
- 7750 SR
 - device support, 13-5
- 7750 SR database
 - backing up, 10-7
 - restoring, 10-7
- 7750 SR security; *See* security for 7750 SR

A

- access egress policies, 20-8
 - creating, 20-22
- access ingress policies, 20-5
 - creating, 20-19
 - fowarding classes, 20-7

- accounting statistics, 30-2
 - log records, 30-4
 - menus, 30-19
 - network performance counters, 30-4
 - procedures, 30-20
 - procedures list, 30-19
 - workflow, 30-18
- alarms; *See* fault management using alarms

B

- BGP, 17-3, 17-3
 - configuring confederation, 17-16
 - configuring global-level, 17-14
 - configuring peer group-level, 17-19
 - configuring peer-level, 17-19
 - enabling on routers, 17-13

C

- cards, 13-8
 - creating daughter, 14-13, 14-13
 - creating type, 14-13, 14-13
- channels
 - about, 13-10
 - configuring SONET clear and STS1 sub-channels, 14-24
 - configuring TDM channels, 14-26
 - SONET sub-channels, 13-13
 - TDM, 13-15

circuit diagnostic — equipment

circuit diagnostic, 29-4
clear channels
 DS3, 13-12
 STS3 to STS192, 13-11
CLI, 12-2
 creating scripts, 12-5
 launching, 12-3
 menus, 12-2
 procedure list, 12-3
 procedures, 12-3
 saving scripts, 12-7
 setting console parameters, 12-4
 using scripts, 12-5
 workflow, 12-2
contextual menus
 navigation tree, 14-3

D

database
 backing up, 11-6
database manager, 11-2
 analyzing database, 11-4
 backing up database, 11-6
 menu, 11-2
 procedures, 11-3
 procedures list, 11-2
 viewing general database statistics, 11-3
 workflow, 11-2
daughter cards, 13-9
 creating, 14-13
deployment and site backup/upgrade, 10-2
 configuring to-node deployment policy,
 10-3
 menu, 10-2
 procedures, 10-3
 procedures list, 10-3
 scheduling node backup, 10-5
 starting immediate backup, 10-7
 starting immediate restore, 10-7
 troubleshooting configuration deployment,
 10-5
 upgrading node software image, 10-8
 viewing backup status, 10-9
 viewing restore status, 10-9

 viewing upgrade status, 10-9
 workflow, 10-2
devices
 7450 ESS, 13-6
 7750 SR, 13-5
 changing configuration from equipment
 manager, 15-9
 changing properties from navigation tree,
 14-10
 discovering, 6-9
 grouping, 14-8
 navigation tree contextual menus, 14-3
 working with, 13-5
diagnostics; *See* fault management using OAM
discovery, 6-2, 6-2
 configuring poller policies, 6-4
 configuring poller SNMPv3, 6-8
 discovering devices, 6-9
 editing discovery rule, 6-14
 managing routers, 6-16
 menus, 6-3
 procedures, 6-4
 procedures list, 6-3
 rescanning network, 6-16
 workflow, 6-3
discovery manager; *See* discovery
discovery rules
 disabling, 6-15
 editing, 6-14
 enabling, 6-15
 removing, 6-16
distributed VPLS, 24-2
drawings
 setting or viewing parameters, 3-6

E

endpoints
 connection termination points, 13-11
equipment
 contextual menus, 14-3
 See also nodes, routers
 viewing alarms for, 28-11

- equipment configuration
 - changing from equipment manager, 15-9
 - configuring Ethernet ports, 14-14
 - configuring SONET clear channels and STS1 sub-channels, 14-24
 - configuring SONET ports, 14-18
 - configuring TDM channels, 14-26
 - configuring TDM ports, 14-23
 - contextual menus, 14-3
 - creating card type, 14-13
 - creating daughter card, 14-13
 - forms, 14-2
 - LAGs, 14-10
- equipment management, 13-2
- equipment manager, 15-2
 - configuring devices, 15-9
 - filtering views, 15-8
 - forms, 15-2
 - menus, 15-8
 - network element filter, 15-8
 - procedures list, 15-8
 - workflow , 15-7
- ethernet ports, 13-12
 - configuring, 14-14
- F**
- FAQs
 - basic troubleshooting, 2-8
- fault management using alarms, 28-2
 - alarm descriptions, 28-20
 - menus, 28-5
 - procedures, 28-6
 - procedures list, 28-5
 - reviewing historical alarms, 28-19
 - setting alarm history behavior, 28-8
 - setting global alarm policies, 28-6
 - setting specific alarms policies, 28-10
 - viewing alarm information, 28-12
 - viewing alarms, 28-11
 - viewing network alarm statistics, 28-19
 - viewing network alarms using dynamic list, 28-17
 - workflow, 28-4
- fault management using OAM, 29-2
 - circuit diagnostic, 29-4
 - interpreting diagnostic results, 29-22
 - LSP ping, 29-4
 - LSP trace, 29-4
 - MAC ping, 29-5
 - MAC populate, 29-6
 - MAC purge, 29-6
 - MAC trace, 29-6
 - menus, 29-8
 - MTU diagnostic, 29-3
 - performing diagnostic from service, 29-13
 - performing diagnostic from service tunnel, 29-9
 - procedures, 29-9
 - procedures list, 29-8
 - tunnel diagnostic, 29-3
 - VPRN ping, 29-7
 - VPRN trace, 29-7
 - workflow, 29-7
- features
 - new, 2-4
- FIB entries
 - managing, 24-38
- filter policies, 20-15
 - creating Acl IP, 20-35
 - creating Acl MAC, 20-36
- Find menu; *See* performing searches
- forms, 4-2
 - arranging work pane, 4-4
 - bringing to foreground, 4-5
 - closing, 4-5
 - equipment manager, 15-2
 - menu options, 4-4
 - setting or viewing parameters, 3-6
- forms management
 - procedures, 4-4
 - procedures list, 4-3
 - workflow, 4-3

G — LSP ping

G

- grouping devices and routers, 14-8
- GUI, 3-2
 - contextual menus navigation tree, 14-3
 - disabling activity check, 3-5
 - enabling activity check, 3-5
 - exiting, 3-11
 - managing lists, 3-9
 - menus, 3-3
 - navigating, 3-6
 - procedures, 3-4
 - procedures list, 3-4
 - starting from PC, 3-4
 - starting from Solaris workstation, 3-5
 - using drawings to set or view parameters, 3-6
 - using forms to set or view parameters, 3-6
 - using menus, 3-5
 - using shortcuts, 3-5
 - using toolbar, 3-5
 - using windows to set or view parameters, 3-6
 - workflow, 3-3

H

- hierarchical schedulers, 20-14
- hierarchical VPLS, 24-4
- HVPLS, 24-2, 24-4
 - creating, 24-35

I

- IES, 25-2
 - creating, 25-6
 - deleting, 25-21
 - modifying, 25-21
- IES management, 25-2
 - menus, 25-5
 - procedures, 25-6
 - procedures list, 25-5
 - sample configuration, 25-3
 - viewing service maps, 25-22
 - workflow, 25-5

- in-band and out-of-band management
 - configuring poller policies, 7-4
 - menu, 7-4
 - procedure, 7-4
 - procedure list, 7-4
 - workflow, 7-3

IS-IS, 17-8

ISIS

- configuring interfaces, 17-40
- configuring NET addresses, 17-39
- configuring router-wide parameters, 17-37
- enabling on routers, 17-36
- planning configuration, 17-36

L

LAGs

- about, 13-7
- creating and configuring, 14-10

LDP, 17-7

- configuring global-level parameters, 17-31
- configuring interfaces, 17-33
- configuring targeted peers, 17-34
- enabling on routers, 17-30
- supported on, 17-30

license key

- viewing, 3-10

lists

- LSPs, 18-16
- LSPs creating, 18-9
- managing, 3-9
- MPLS paths, 18-15
- saving preferences, 3-10
- service tunnels, 19-6
- viewing, 3-9

local VPLS, 24-2

logical components

- viewing alarms for, 28-11

LSP map, 27-2

LSP path map, 27-3

- opening from LSP Path Manager, 27-9
- opening from MPLS Path Manager, 27-9

LSP paths

- configuring, 18-14

LSP ping, 29-4

LSP trace, 29-4

LSPs

creating, 18-9

M

MAC address

VPLS, 24-2

MAC OAM

MAC populate and MAC purge, 29-13

MAC ping, 29-5

MAC populate

performing, 29-13

MAC populate , 29-6

MAC purge, 29-6

performing, 29-13

MAC trace, 29-6

map management, 27-2

menus, 27-7

procedures, 27-8

procedures list, 27-7

workflow, 27-7

maps

listing object information, 27-10

LSP, 27-2

LSP path, 27-3

opening, 27-8

opening LSP path from LSP Path Manager,
27-9

opening LSP path from MPLS Path
Manager, 27-9

service, 27-4

service path, 27-6

viewing elements, 27-8

viewing for services, 23-21

viewing LSPs, 18-16

viewing object information, 27-10

zooming in, 27-10

zooming out, 27-10

MIBs

SNMP, 6-18

MP-BGP, 17-3

MPLS

configuring administrative group policy,
16-16

MPLS configuration, 18-2

configuring LSP paths, 18-14

creating interfaces, 18-5

creating LSPs, 18-9

creating paths, 18-7

enabling on routing instance, 18-5

listing LSPs, 18-16

listing paths, 18-15

menus, 18-4

procedures, 18-5

procedures list, 18-4

viewing LSP map, 18-16

workflow, 18-4

MTU diagnostic, 29-3

MTU ping

performing, 29-9

N

naming conventions

SONET channels, 13-13

TDM channels, 13-15

navigation tree, 14-2

changing device properties, 14-10

configuring Ethernet ports, 14-14

configuring LAGs, 14-10

configuring SONET clear channels and
STS1 sub-channels, 14-24

configuring SONET ports, 14-18

configuring TDM channels, 14-26

configuring TDM ports, 14-23

contextual menus, 14-3

creating a card type, 14-13

creating a daughter card, 14-13

equipment menus, 14-7

grouping devices and routers, 14-8

procedures list, 14-7

workflow to manage equipment, 14-7

network element filter, 15-8

network faults

workflow using alarms, 28-4

network hierarchy, 14-2

network maps; *See* maps

network object

working with, 13-4

network policies — poller policies

- network policies, 20-9
 - creating, 20-24
- network queue policies, 20-10
 - creating, 20-27
- nodes
 - scheduling backups, 10-5
 - See also* routers
 - upgrading software image, 10-8
- O**
- OAM; *See* fault management using OAM
- objects
 - about, 13-3
 - cards and card slots, 13-8
 - changing device properties from
 - navigation tree, 14-10
 - channels, 13-10
 - creating, 13-4
 - daughter cards, 13-9
 - devices, 13-5
 - grouping devices, 14-8
 - LAGs, 13-7
 - network, 13-4
 - ports, 13-10
 - shelves, 13-8
- OSPF, 17-5
 - adding router to area, 17-28
 - configuring area, 17-25
 - configuring on routers, 17-24
 - creating a virtual link, 17-30
 - enabling on routers, 17-23
 - planning configuration, 17-22
- out-of-band management; *See* in-band and out-of-band management
- P**
- passwords
 - changing as system administrator, 8-9
 - changing as user, 8-9
- paths
 - creating MPLS, 18-7
- performance monitoring statistics, 30-2
 - creating accounting policy, 30-22
 - creating file policy, 30-20
 - menus, 30-19
 - modifying accounting policy, 30-22
 - modifying equipment statistics, 30-26
 - modifying file policy, 30-20
 - modifying object-based statistics, 30-26
 - procedures, 30-20
 - procedures list, 30-19
 - See also* accounting statistics
 - types, 30-3
 - viewing equipment statistics, 30-25
 - viewing object-based statistics, 30-25
 - viewing statistics logs, 30-28
 - workflow, 30-18
- performing searches, 5-2
 - menu, 5-2
 - procedures, 5-3
 - procedures list, 5-3
 - using Find menu, 5-3
 - using Search button, 5-5
 - using Select button, 5-6
 - workflow, 5-2
- permissions, 8-3
- policies, 20-2
 - access egress, 20-8
 - access ingress, 20-5
 - copying, 20-40
 - deleting, 20-39
 - distributing, 20-38
 - editing, 20-39
 - filter, 20-15
 - network, 20-9
 - network queue, 20-10
 - overwriting, 20-40
 - removing unassociated, 20-41
 - scheduler, 20-13
 - service management, 20-5
 - setting for global alarms, 28-6
 - setting for specific alarms, 28-10
 - slope, 20-11
 - synchronizing, 20-40
- poller policies
 - configuring for network elements, 6-4
 - configuring for SNMPv3 security, 6-8
 - configuring in-band and out-of-band, 7-4

ports

- about, 13-10
- configuring Ethernet ports, 14-14
- configuring SONET ports, 14-18
- configuring TDM ports, 14-23
- ethernet ports, 13-12

R

RIP, 17-5

- configuring global-level, 17-20
- configuring group-level, 17-21
- configuring interface-level, 17-22

router configuration, 16-2

- configuring Layer 3 interface, 16-7
- configuring MPLS administrative group policy, 16-16
- configuring router routing instance parameters, 16-5
- configuring routing policy, 16-11
- configuring static route, 16-18
- menus, 16-4
- modifying Layer 3 interface, 16-7
- procedures, 16-5
- procedures list, 16-5
- workflow, 16-3

routers

- grouping, 14-8
- managing, 6-16
- reconciling elements, 6-17
- unmanaging, 6-16

routing protocol configuration, 17-2

- adding Layer 3 interfaces to OSPF area, 17-25
- adding router to OSPF area, 17-28
- configuring BGP confederation, 17-16
- configuring global-level BGP, 17-14
- configuring global-level LDP parameters, 17-31
- configuring global-level RIP, 17-20
- configuring group-level RIP, 17-21
- configuring interface-level RIP, 17-22
- configuring ISIS interfaces, 17-40
- configuring ISIS NET addresses, 17-39
- configuring LDP interfaces, 17-33

- configuring LDP targeted peers, 17-34
- configuring OSPF area, 17-25
- configuring OSPF on routers, 17-24
- configuring peer group-level BGP, 17-19
- configuring peer-level BGP, 17-19
- configuring router-wide ISIS parameters, 17-37
- creating a virtual link, 17-30
- enabling BGP on routers, 17-13
- enabling ISIS on routers, 17-36
- enabling LDP on routers, 17-30
- enabling OSPF on routers, 17-23
- menus, 17-11
- procedures, 17-12
- procedures list, 17-11
- workflow, 17-10

routing protocols

- BGP, 17-3
- IS-IS, 17-8
- LDP, 17-7
- MP-BGP, 17-3, 17-3
- OSPF, 17-5
- RIP, 17-5

S

scheduler policies

- creating, 20-32
- hierarchical, 20-14
- single tier, 20-14

SDP; *See* service tunnelssearches; *See* performing searches

security for 5620 SAM

- changing user passwords as system administrator, 8-9
- changing user passwords as user, 8-9
- configuration group procedures, 8-5
- configuration group procedures list, 8-4
- configuration user procedures, 8-5
- configuration user procedures list, 8-4
- creating user accounts, 8-6, 8-6
- creating user groups, 8-5
- deleting groups, 8-7
- deleting user accounts, 8-8
- permissions, 8-3

security for 5620 SAM (continued) — statistics

- reinstating users, 8-8
- suspending users, 8-8
- workflow for groups, 8-4
- workflow for users, 8-4
- security for 7750 SR, 9-2
 - creating RADIUS access policies, 9-13
 - creating site management access filter policies, 9-5
 - creating TACACS+ access policies, 9-14
 - creating user accounts, 9-9
 - creating user profiles, 9-8
 - distributing policies, 9-16
 - managing user accounts, 9-9
 - menus, 9-4
 - modifying password policies, 9-12
 - modifying site management access filter policies, 9-5
 - procedures, 9-5
 - procedures list, 9-4
 - RADIUS policies and permissions, 9-3
 - specifying password policies, 9-12
 - TACACS+ policies and permissions, 9-3
 - user and group permissions, 9-3
 - workflow, 9-3
- service, 27-4
- service management, 22-2
 - access interfaces, 22-6
 - sample HQoS network configuration, 22-7
- service management policies, 20-5
 - access egress, 20-8
 - access ingress, 20-5
 - copying, 20-40
 - creating access egress, 20-22
 - creating access ingress, 20-19
 - creating Acl IP filter, 20-35
 - creating Acl MAC filter, 20-36
 - creating aggregation scheduler, 20-34
 - creating network, 20-24
 - creating network queue, 20-27
 - creating scheduler, 20-32
 - creating slope, 20-25
 - deleting, 20-39
 - distributing, 20-38
 - editing, 20-39
 - filter, 20-15
 - menu, 20-17
 - network, 20-9
 - network queue, 20-10
 - overwriting, 20-40
 - procedures, 20-19
 - procedures list, 20-18
 - removing unassociated, 20-41
 - scheduler, 20-13
 - slope, 20-11
 - synchronizing, 20-40
 - workflow, 20-17
- service path, 27-6
- service tunnels, 19-2
 - configuring, 19-4
 - listing, 19-6
 - menus, 19-3
 - procedures, 19-4
 - procedures list, 19-3
 - viewing map, 19-6
- services
 - configuration workflow, 1-2
 - management workflow, 1-2
 - viewing alarms for, 28-11
- shelves
 - about, 13-8
- single tier schedulers, 20-14
- slope policies, 20-11
 - creating, 20-25
- SNMP MIBs, 6-18
- SNMPv3 security, 6-8
- software release
 - viewing, 3-10
- SONET ports
 - configuring, 14-18
 - configuring clear channels and STS1 sub-channels, 14-24
- spoke access circuits
 - creating, 24-35
- SSH session, 12-2
- statistics
 - accounting, 30-2
 - performance monitoring, 30-3
 - viewing for database, 11-3
 - viewing for network alarms, 28-19

subscriber configuration, 21-2
 menu, 21-3
 procedures, 21-3
 procedures list, 21-3
 workflow, 21-2

subscribers, 21-2
 creating, 21-4
 deleting, 21-7
 managing information, 21-5
 maps, 21-7

T

TDM channels

 configuring, 14-26

TDM ports

 configuring, 14-23

Telnet session, 12-2

topology maps; *See* maps

troubleshooting

 basic FAQs, 2-8

 configuration deployment, 10-5

 using alarms, 28-2

 using OAM, 29-2

 VPRN, 26-4

tunnel diagnostic, 29-3

tunnel ping

 performing, 29-9

V

views

 filtering using equipment manager, 15-8

VLL

 spoke access circuits, 24-35

VLL service, 23-2

 creating, 23-7

 deleting, 23-21

 modifying, 23-20

VLL service management, 23-2

 menus, 23-6

 procedures, 23-7

 procedures list, 23-7

 sample configuration, 23-4

 viewing service map, 23-21

 workflow, 23-6

VPLS, 24-2

 creating, 24-15

 creation workflow, 24-13

 deleting, 24-34

 distributed, 24-2

 local, 24-2

 MAC address learning, 24-2

 modifying, 24-33

 spoke access circuits, 24-35

 STP, 24-2

VPLS management, 24-2

 managing FIB entries, 24-38

 menus, 24-14

 procedures, 24-14

 procedures list, 24-14

 sample configuration, 24-7

 viewing service maps, 24-40

 workflow, 24-13

VPRN ping, 29-7

VPRN policies, 26-4

VPRN service, 26-2

 creating, 26-8

 deleting, 26-33

 modifying, 26-33

VPRN service management, 26-2

 menus, 26-7

 procedures, 26-8

 procedures list, 26-7

 sample configuration, 26-4

 viewing service maps, 26-34

 workflow, 26-6

VPRN service routers, 26-3

VPRN trace, 29-7

VPRN troubleshooting, 26-4

W

windows

 setting or viewing parameters, 3-6

