Alcatel-Lucent 5620

SERVICE AWARE MANAGER | RELEASE 8.0 R5

TROUBLESHOOTING GUIDE

3HE 05723 AAAE TQZZA Edition 01

Disclaimers

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

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

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

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

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

Alcatel-Lucent License Agreement

SAMPLE END USER LICENSE AGREEMENT

1. LICENSE

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

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

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

2. PROTECTION AND SECURITY OF LICENSED PROGRAMS

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

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

3. TERM

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

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

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

4. CHARGES

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

5. SUPPORT AND UPGRADES

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

6. WARRANTIES AND INDEMNIFICATION

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

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

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

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

7. LIMITATION OF LIABILITY

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

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

8. GENERAL

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

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

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

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

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

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

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

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

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

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

Preface

The Preface provides general information about the 5620 Service Aware Manager documentation suite.

Note — You can use the Search function of Acrobat Reader (File→Search) to find a term in a PDF of this document. To refine your search, use appropriate search options (for example, search for whole words only or enable case-sensitive searching). You can also search for a term in multiple PDFs at once. For more information, see the Help for Acrobat Reader.

5620 SAM documentation suite

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

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

Table 1 5620 SAM customer documentation suite

Guide	Description
5620 SAM core documentation	
5620 SAM | 5650 CPAM Installation and Upgrade Guide	The *5620 SAM | 5650 CPAM Installation and Upgrade Guide* provides OS considerations, configuration information, and procedures for the following: • installing, upgrading, and uninstalling 5620 SAM and 5650 CPAM software in standalone and redundant deployments • 5620 SAM system migration to a different system • conversion from a standalone to a redundant 5620 SAM system

(1 of 3)

Guide	Description
5620 SAM User Guide	The *5620 SAM User Guide* provides information about using the 5620 SAM to manage the service-aware IP/MPLS network, including GUI basics, commissioning, service configuration, and policy management. The *5620 SAM User Guide* uses a task-based format. Each chapter contains: • a workflow that describes the steps for configuring and using the functionality • detailed procedures that list the configurable parameters on the associated forms 5620 SAM management information specific to LTE network elements is covered in the *5620 SAM LTE ePC User Guide* and *5620 SAM LTE RAN User Guide*.
5620 SAM Parameter Guide	The *5620 SAM Parameter Guide* provides: • parameter descriptions that include value ranges and default values • parameter options and option descriptions • parameter and option dependencies • parameter mappings to the 5620 SAM-O XML equivalent property names There are dynamic links between the procedures in the *5620 SAM User Guide* and the parameter descriptions in the *5620 SAM Parameter Guide*. See Procedure 2 for more information. Parameters specific to LTE network elements are covered in the *5620 SAM LTE Parameter Reference*.
5620 SAM Statistics Management Guide	The *5620 SAM Statistics Management Guide* provides information about how to configure performance and accounting statistics collection and how to view counters using the 5620 SAM. Network examples are included.
5620 SAM Scripts and Templates Developer Guide	The *5620 SAM Scripts and Templates Developer Guide* provides information that allows you to develop, manage, and execute CLI-based or XML-based scripts or templates. The guide is intended for developers, skilled administrators, and operators who are expected to be familiar with the following: • CLI scripting, XML, and the Velocity engine • basic scripting or programming • 5620 SAM functions

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

5620 SAM Maintenance Guide	The *5620 SAM Maintenance Guide* provides procedures for: • generating baseline information for 5620 SAM applications • performing daily, weekly, monthly, and as-required maintenance activities for 5620 SAM-managed networks
5620 SAM Integration Guide	The *5620 SAM Integration Guide* provides procedures to allow the 5620 SAM to integrate with additional components.
5620 SAM System Architecture Guide	The *5620 SAM System Architecture Guide* is intended for technology officers and network planners to increase their knowledge of the 5620 SAM software structure and components. It describes the system structure, software components, and interfaces of the 5620 SAM. In addition, 5620 SAM fault tolerance, security, and network management capabilities are discussed from an architectural perspective.

(2 of 3)

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

(3 of 3)

Procedure 1 To find the 5620 SAM user documentation

The user documentation is available from the following sources:

- the User_Documentation directory on the product DVD-ROM
- Help→5620 SAM User Documentation in the 5620 SAM client GUI main menu

Note — Users of Mozilla browsers may receive an error message when using the User Documentation Index page (index.html) to open the PDF files in the 5620 SAM documentation suite. The offline storage and default cache values used by the browsers are the cause of the error message.

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

Procedure 2 To view parameter descriptions from the *5620 SAM User Guide*

You can click on a parameter name in a *5620 SAM User Guide* procedure to open the matching parameter description in the *5620 SAM Parameter Guide*. Ensure the following conditions are true beforehand:

- the *5620 SAM Parameter Guide* and *5620 SAM User Guide* are located in the same directory
- Adobe Reader Release 5.0 or later is installed

1 To view a parameter description when both the *5620 SAM User Guide* and the *5620 SAM Parameter Guide* are open in Adobe Acrobat, click on the parameter name in the *5620 SAM User Guide*.

The parameter description is displayed in the *5620 SAM Parameter Guide*.

2 To view a parameter description when only the *5620 SAM User Guide* is open in Adobe Acrobat:

i Click on a parameter name in a procedure in the *5620 SAM User Guide*. The *5620 SAM User Guide* closes and the *5620 SAM Parameter Guide* opens to display the parameter description.

ii Double-click on the Previous View button in Adobe Acrobat (or press Alt + ←) to re-open the *5620 SAM User Guide*. The *5620 SAM User Guide* opens and displays the parameter from step i.

Prerequisites

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

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

Conventions

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

Table 2 Documentation conventions

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

Measurement conventions

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

Table 3 lists the measurement symbols used in this document.

Table 3 Bits and bytes conventions

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

Important information

The following conventions are used to indicate important information:

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

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

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

Contents

Troubleshooting overview

1 — Troubleshooting process

1.1 Troubleshooting process

The troubleshooting process identifies and resolves performance issues related to a network service or component. The performance issue can be an intermittent or a continuous degradation in service, or a complete network failure.

The first step in problem resolution is to identify the problem. Problem identification can include an alarm received from a network component, an analysis of network capacity and performance data, or a customer problem report.

The personnel responsible for troubleshooting the problem must:

- understand the designed state and behavior of the network, and the services that use the network
- recognize and identify symptoms that impact the intended function and performance of the product

Network maintenance

The most effective method to prevent problems is to schedule and perform routine maintenance on your network. Major networking problems often start as minor performance issues. See the *5620 SAM Maintenance Guide* for more information about how to perform routine maintenance on your network.

1.2 Troubleshooting problem-solving model

An effective troubleshooting problem-solving model includes the following tasks:

1. Establish a performance baseline.
2. Categorize the problem.
3. Identify the root cause of the problem.
4. Plan corrective action and resolve the problem.
5. Verify the solution to the problem.

See General Procedure 2.3 for information on how the problem-solving model aligns with using the 5620 SAM to troubleshoot your network or network management problem.

Establish a performance baseline

You must have a thorough knowledge of your network and how it operates under normal conditions to troubleshoot problems effectively. This knowledge facilitates the identification of fault conditions in your network. You must establish and maintain baseline information for your network and services. The maintenance of the baseline information is critical because a network is not a static environment.

See the *5620 SAM Maintenance Guide* for more information on how to generate baseline information for 5620 SAM applications.

Categorize the problem

When you categorize a problem, you must differentiate between total failures and problems that result in a degradation in performance. For example, the failure of an access switch results in a total failure for a customer who has one DS3 link into a network. A core router that operates at over 80% average utilization can start to discard packets, which results in a degradation of performance for some applications that use the device. Performance degradations exhibit different symptoms from total failures and may not generate alarms or significant network events.

Multiple problems can simultaneously occur and create related or unique symptoms. Detailed information about the symptoms that are associated with the problem helps the NOC or engineering operational staff diagnose and fix the problem. The following information can help you assess the scope of the problem:

- alarm files
- error logs
- network statistics
- network analyzer traces
- output of CLI show commands
- accounting logs
- customer problem reports

Use the following guidelines to help you categorize the problem:

- Is the problem intermittent or static?
- Is there a pattern associated with intermittent problems?
- Is there an alarm or network event that is associated with the problem?
- Is there congestion in the routers or network links?
- Has there been a change in the network since proper function?

Identify the root cause of the problem

A symptom for a problem can be the result of more than one network issue. You can resolve multiple, related problems by resolving the root cause of the problem. Use the following guidelines to help you implement a systematic approach to resolve the root cause of the problem:

- Identify common symptoms across different areas of the network.
- Focus on the resolution of a specific problem.
- Divide the problem based on network segments and try to isolate the problem to one of the segments. Examples of network segments are:
  - LAN switching (edge access)
  - LAN routing (distribution, core)
  - metropolitan area
  - WAN (national backbone)
  - partner services (extranet)
  - remote access services
- Determine the network state before the problem appeared.
- Extrapolate from network alarms and network events the cause of the symptoms. Try to reproduce the problem.

The following 5620 SAM features can help you identify the root cause of a problem:

- alarms with vendor-specific and X.733 standardized probable causes
- alarm history associated network conditions

Plan corrective action and resolve the problem

The corrective action required to resolve a problem depends on the problem type. The problem severity and associated QoS commitments affect the approach to resolving the problem. You must balance the risk of creating further service interruptions against restoring service in the shortest possible time. Corrective action should:

1. Document each step of the corrective action.
2. Test the corrective action.
3. Use the CLI to verify behavior changes in each step.
4. Apply the corrective action to the live network.
5. Test to verify that the corrective action resolved the problem.

Verify the solution to the problem

You must make sure that the corrective action associated with the resolution of the problem did not introduce new symptoms in your network. If new symptoms are detected, or if the problem has only recently been mitigated, you need to repeat the troubleshooting process.

1.3 Troubleshooting guidelines

When a problem is identified in the network management domain, track and store data to use for troubleshooting purposes:

- Determine the type of problem by reviewing the sequence of events before the problem occurred:
  - Trace the actions that were performed to see where the problem occurred.
  - Identify what changed before the problem occurred.
  - Determine whether the problem happened before under similar conditions.
- Check the documentation or your procedural information to verify that the steps you performed followed documented standards and procedures.
- Check the alarm log for any generated alarms that are related to the problem.
- Record any system-generated messages, such as error dialog boxes, for future troubleshooting.
- If you receive an error message, perform the actions recommended in the error dialog box, client GUI dialog box, SOAP exception response, or event notification.

During troubleshooting:

- Keep both the Alcatel-Lucent documentation and your company policies and procedures nearby.
- Check the appropriate release notice from the Support Documentation Service at https://www.alcatel-lucent.com/support for any release-specific problems, restrictions, or usage recommendations that relate to your problem.
- If you need help, confirmation, or advice, contact your TAC or technical support representative. See Table 1-1 to collect the appropriate information before you call support.
- Contact your TAC or technical support representative if your company guidelines conflict with Alcatel-Lucent documentation recommendations or procedures.
- Perform troubleshooting based on your network requirements.

1.4 Before you call support

Collect the information listed in Table 1-1 before you call your TAC or technical support representative.

The list of Alcatel-Lucent support contacts is available from the Alcatel-Lucent home page at http://www.alcatel-lucent.com/support.

Table 1-1 Troubleshooting data collection for support

Action	Collect the following
Collect software and platform information	• release version and load of the 5620 SAM software • Solaris or Windows operating system version and patch set • platform information, including CPU, disk, and RAM data See Procedure 2-1 for more information.
Collect required software logs	• relevant log files from the PC or workstation on which the problem occurs. For example, for problems on a main or auxiliary server, retrieve the EmsServer.log or AuxServer.log file from the *installation_directory*/nms/log directory or folder. On a Solaris station, you can run a log-file collection utility. See Procedure 2-1 for more information.
Collect information about actions performed before the problem occurred	• if appropriate, screen captures or a text version of the error or exception message received • an inventory of the actions; for example, the GUI configurations performed before the problem occurred • any troubleshooting actions and the results

2 — 5620 SAM troubleshooting

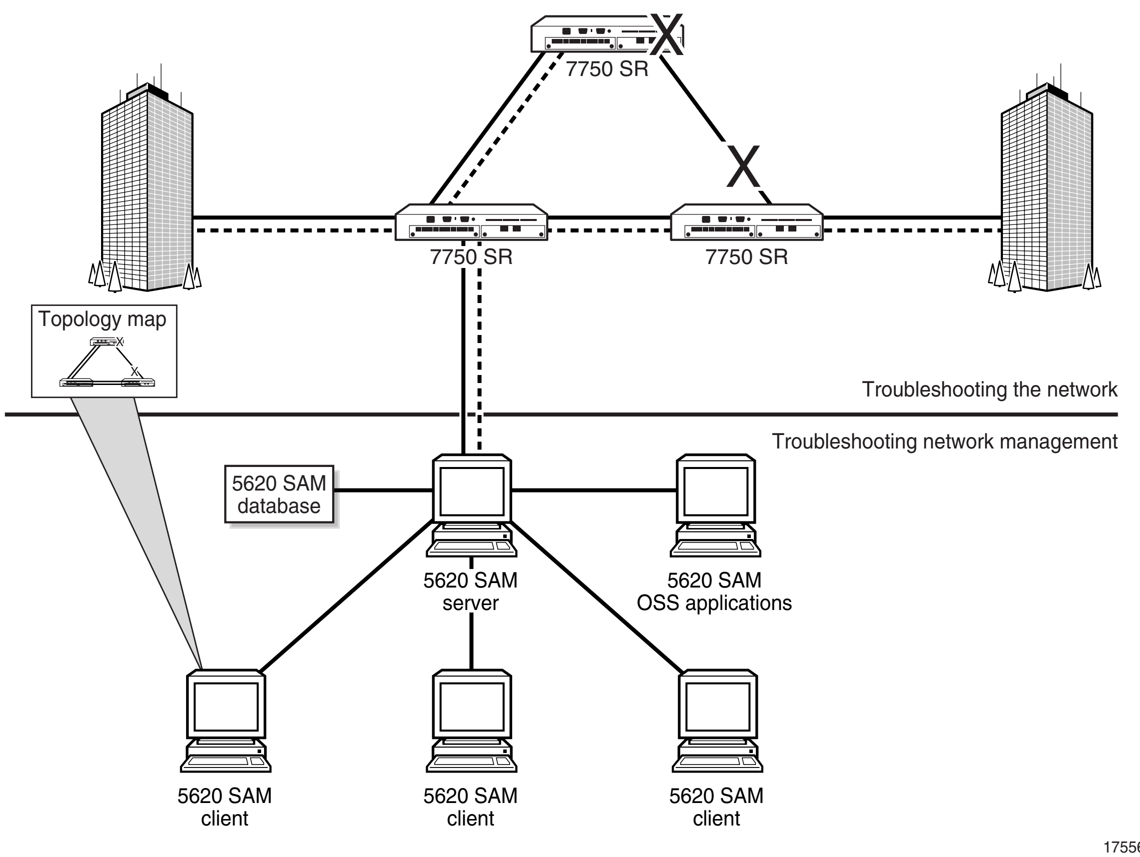
2.1 5620 SAM troubleshooting process

The *5620 SAM Troubleshooting Guide* is intended for NOC operators and other engineering operational staff who are responsible for identifying and resolving performance issues in a 5620 SAM network. This guide contains describes the following general troubleshooting types:

- managed-NE network troubleshooting
- network management domain troubleshooting

Figure 2-1 shows the 5620 SAM troubleshooting types.

Figure 2-1 5620 SAM troubleshooting types



Troubleshooting the managed-NE network

You can use the 5620 SAM alarm and service monitoring functions to help you troubleshoot the network of managed NEs.

Alarms for network objects

The 5620 SAM converts SNMP traps from NEs to events and alarms. You can then use the 5620 SAM to correlate the events and alarms to the managed object, configured services and policies. A correlated event or alarm can cause fault conditions on multiple network objects and services. For example, an alarm raised for a port failure causes alarms on all services that use that port. You can view the alarm notification from the 5620 SAM topology maps, service configuration forms, and customer information form that lists the affected objects.

See chapters 3 and 5 for more information about using the 5620 SAM alarm information to troubleshoot a network.

Service problems with no associated alarms

The proper delivery of services requires a number of operations that must occur correctly at different levels within the service model. For example, an operation such as the association of packets to a service, VC labels to a service, and each service to a service tunnel must be performed successfully for the service to pass traffic according to SLAs.

Even when tunnels are operating correctly and are correctly bound to services, for example, incorrect FIB information can cause connectivity issues. You can use configurable in-band or out-of-band packet-based OAM tools to verify that a service is operational and that the FIB information is correct. Each OAM diagnostic can test each of the individual packet operations. You must test the packet operation in both directions.

For in-band, packet-based testing, the OAM packets closely resemble customer packets to effectively test the forwarding path for the customer. However, you can distinguish the OAM packets from customer packets, so they remain within the managed network and are not forwarded to the customer. For out-of-band testing, OAM packets are sent across some portion of the transport network. For example, OAM packets are sent across LSPs to test reachability.

See chapter 4 for more information about using the 5620 SAM service information to troubleshoot your network.

Troubleshooting the network management domain

Troubleshooting the network management domain is a reactive fault-management process that requires comprehensive knowledge of the following:

- 5620 SAM database, 5620 SAM main and auxiliary servers, the 5620 SAM-O interface, and the 5620 SAM client software
- Windows and Solaris operating systems
- Windows PC and Solaris workstations
- TCP/IP networking

Note — Unless specified otherwise, the term “server” in this document refers to a 5620 SAM main server to which 5620 SAM clients connect.

2.2 5620 SAM troubleshooting tools

The 5620 SAM supports the use of OAM diagnostic tools and event logs to help identify the root cause of a network or network management problem.

OAM diagnostics

The 5620 SAM supports configurable in-band and out-of-band, packet-based OAM diagnostic tools to troubleshoot your network service. See "STM OAM diagnostics for troubleshooting" in section 4.1 for more information.

Log files

You can use log files to help troubleshoot your network.

The 5620 SAM log files can consume large amounts of disk space when a system runs for a long period with significant activity. Ensure that the contents of the various log directories are backed up on a regular basis. See the *5620 SAM Maintenance Guide* for more information about how to perform routine 5620 SAM system maintenance. See Procedure 2-1 for information about collecting 5620 SAM log files.

Note — The event log files may be overwritten or removed when you restart a 5620 SAM station.

2.3 Workflow for 5620 SAM troubleshooting

The following is the high-level sequence of actions to perform with respect to the problem-solving model described in section 1.2.

1 Establish an operational baseline for your network. See the *5620 SAM Maintenance Guide* for more information.

2 When a problem occurs, identify the type of problem. Table 2-1 lists and describes the 5620 SAM troubleshooting types.

Table 2-1 5620 SAM general troubleshooting type descriptions

Type	Example problems
Managed NE network	• Operational issue with the network managed by 5620 SAM • Alarms raised on network objects and services • Problems on services with no associated alarms • Topology maps indicate problems

(1 of 2)

Type	Example problems
Network management domain	• A domain, connectivity, platform, or configuration problem • Network management domain and LAN troubleshooting • Platform troubleshooting • 5620 SAM GUI and OSS client software issues • 5620 SAM main or auxiliary server software issues • 5620 SAM database and Oracle software issues • Warning messages related to configuration • Problems Encountered form displayed in client GUI • 5620 SAM user session or NE deployment problems

(2 of 2)

3 Identify the root cause of the problem and plan corrective action.

a For a managed-network problem, perform one of the following procedures:

- 3.2 to investigate and resolve alarm conditions on a network object or customer service
- 4.2 to detect and resolve problems on customer services that have no associated alarms

Note — See chapter 5 for information about using topology maps to monitor and troubleshoot the managed network.

b For a network management domain problem, use Table 2-2 to identify the appropriate troubleshooting procedure for the problem.

Table 2-2 5620 SAM network management problems

Problem	Solution
General	
To collect the 5620 SAM log files	Procedure 2-1
Troubleshooting network management LAN problems	
Problem: All network management domain PCs and workstations are experiencing performance degradation	Procedure 7-1
Problem: Lost connectivity to one or more network management domain PCs or workstations	Procedure 7-2
Problem: Another machine can be pinged, but some functions are unavailable	Procedure 7-3
Problem: Packet size and fragmentation issues	Procedure 7-4
Troubleshooting Solaris and Windows platforms	
Problem: Slow processing on a Solaris workstation and CPU peaks	Procedure 8-1
Problem: Slow performance on a Solaris workstation, but no spike or peak in the CPU	Procedure 8-2
Problem: There is excess disk activity on my Solaris platform	Procedure 8-3
Problem: There is not enough swap space added or the Solaris platform is disk bound	Procedure 8-4
General information about troubleshooting the Windows platform	Section 8.2
Troubleshooting 5620 SAM client GUIs and client OSS applications	
Problem: Delayed server response to client activity	Procedure 9-3
Problem: Unable to print from Solaris platform client	Procedure 9-5
Problem: Cannot place newly discovered device in managed state	Procedure 9-6
Problem: I performed an action, such as saving a configuration, but I cannot see any results	Procedure 9-7
Problem: Device configuration backup not occurring	Procedure 9-8
Problem: 5620 SAM client unable to communicate with 5620 SAM server	Procedure 9-2
Problem: Cannot start 5620 SAM client, or error message during client startup	Procedure 9-1
Problem: Cannot view 5620 SAM alarms using 5620 NM client	Procedure 9-4

(1 of 3)

Problem	Solution
Problem: 5620 SAM client GUI shuts down regularly	Procedure 9-9
Problem: Configuration change not displayed on 5620 SAM client GUI	Procedure 9-10
Problem: List or search function takes too long to complete	Procedure 9-11
Problem: Cannot select certain menu options or cannot save certain configurations	Procedure 9-12
Problem: Cannot open user documentation from 5620 SAM client GUI	Procedure 9-14
Troubleshooting 5620 SAM server issues	
Problem: Cannot manage new devices	Procedure 10-9
Problem: A 5620 SAM server cannot be reached over a network	Procedure 10-5
Problem: Excessive 5620 SAM server-to-client response time	Procedure 10-6
Problem: Cannot start a 5620 SAM server, or unsure of 5620 SAM server status	Procedure 10-1
Problem: All SNMP traps from managed devices are arriving at one 5620 SAM server, or no SNMP traps are arriving	Procedure 10-8
Problem: Cannot discover more than one device, or device resynchronization fails	Procedure 10-10
Problem: A 5620 SAM server starts up, and then quickly shuts down	Procedure 10-3
Problem: Unable to receive alarms on the 5620 NM from the 5620 SAM	Procedure 10-13
Problem: Unable to receive alarms on the 5620 SAM, or alarm performance is degraded	Procedure 10-7
Problem: 5620 SAM server and database not communicating	Procedure 10-2
Problem: Statistics are rolling over too quickly	Procedure 10-12
Problem: Slow or failed resynchronization with network devices	Procedure 10-11
Troubleshooting the 5620 SAM database	
Problem: The database is running out of disk space	Procedure 11-2
Problem: A short database backup interval is creating database performance issues	Procedure 11-3
Problem: Database corruption or failure	Procedure 11-1
Problem: A database restore fails and generates a No backup sets error	Procedure 11-4
Problem: Database redundancy failure	Procedure 11-5
Problem: Primary or standby database is down	Procedure 11-6
Problem: Need to verify that Oracle database and listener services are started	Procedure 11-7
Problem: Need to determine status or version of database or Oracle proxy	Procedure 11-8
Troubleshoot using the GUI warning messages	
To respond to a warning message	Procedure 12-1
Troubleshoot with Problem Encountered forms	
To view additional problem information	Procedure 13-1
To collect problem information for technical support	Procedure 13-2
Troubleshoot with the client activity log	

(2 of 3)

Problem	Solution
To identify the user associated with a network problem	Procedure 14-1
To identify the database activity for a user request	Procedure 14-2
To identify the deployment results for a user request	Procedure 14-3
To retrieve historical user logs	Procedure 14-4

(3 of 3)

4 Verify the solution.

2.4 5620 SAM troubleshooting procedures

Use the following procedures for general 5620 SAM network troubleshooting.

Procedure 2-1 To collect the 5620 SAM log files

Perform this procedure to collect the relevant log files for troubleshooting a 5620 SAM database, server, or client problem.

Note — After a system restart, 5620 SAM log files are backed up to directories that are named using a timestamp. A component that runs for a long time can generate multiple log files. Before you restart a 5620 SAM component, ensure that there is sufficient disk space to store the backed up log files.

1 If the problem is related to a 5620 SAM installation, perform the following steps.

i Collect the following files from the /tmp directory on Solaris or the C:\tmp directory on Windows:

- 5620_SAM_*component*_Install_stderr.txt
- 5620_SAM_*component*_Install_stdout.txt

where *component* is the 5620 SAM component name, for example, dbconfig, 5620_SAM_5650_CPAM_Server, or Client

ii Navigate to the *install_dir* directory, where *install_dir* is the component installation location, typically one of the following:

- database—/opt/5620sam/samdb/install on Solaris or C:\5620sam\samdb\install on Windows
- main server—/opt/5620sam/server on Solaris or C:\5620sam\server on Windows
- auxiliary server—/opt/5620sam/auxserver on Solaris or C:\5620sam\auxserver on Windows
- single-user client or client delegate server—/opt/5620sam/client on Solaris or C:\5620sam\client on Windows

iii Collect the following files from the *install_dir* directory:

- 5620_SAM_*component*.install.*time*.stderr.txt
- 5620_SAM_*component*.install.*time*.stdout.txt
- 5620_SAM_*component*_InstallLog.log

where
component is the 5620 SAM component name, for example, Database_Configurator, Server, or Client
time is the installation start time

2 For a Solaris database problem that is not related to installation, collect the following files:

- *install_dir*/admin/*db_instance*/bdump/alert_*db_instance*.log
- *install_dir*/admin/*db_instance*/proxy/OracleProxyLog.txt
- *install_dir*/config/dbconfig.properties
- all files with a .log extension in the following directories:
  - *install_dir*
  - *install_dir*/config

where

install_dir is the database installation location, typically /opt/5620sam/samdb/install

db_instance is the database instance name, typically samdb in a standalone deployment, or samdb1 or samdb2 in a redundant deployment

3 For a Windows database problem that is not related to installation, collect the following files:

- *install_dir*\admin*db_instance*\bdump\alert_*db_instance*.log
- *install_dir*\admin*db_instance*\proxy\OracleProxyLog.txt
- *install_dir*\config\dbconfig.properties
- all files in the following directories that have a .log extension:
  - *install_dir*
  - *install_dir*\config

where

install_dir is the database installation location, typically C:\5620sam\samdb\install

db_instance is the database instance name, typically samdb

4 For a Solaris main or auxiliary server problem that is not related to installation, collect all files with a .log extension in the following directories:

- *install_dir*/nms/log
- *install_dir*/nms/jboss/server/default/log
- *install_dir*/nms/jboss/server/jms/log

where *install_dir* is the server installation location, typically /opt/5620sam/server for a main server, and /opt/5620sam/auxserver for an auxiliary server

5 For a Windows main server problem that is not related to installation, collect all files with a .log extension in the following directories:

- *install_dir*\nms\log
- *install_dir*\nms\jboss\server\default\log
- *install_dir*\nms\jboss\server\jms\log

where *install_dir* is the server installation location, typically C:\5620sam\server

6 For a Solaris single-user client or client delegate server problem that is not related to installation, collect the following files:

- *install_dir*/nms/config/nms-client.xml
- all files and subdirectories in the *install_dir*/nms/log/client directory

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

7 For a Windows single-user client problem that is not related to installation, collect the following files:

- *install_dir*\nms\config\nms-client.xml
- all files and subdirectories in the *install_dir*\nms\log\client directory

where *install_dir* is the client software installation location, typically C:\5620sam\client

8 If required, you can run the getDebugFiles.bash utility on a Solaris station to collect a comprehensive group of troubleshooting log files for use by Alcatel-Lucent technical support.

i Log in to the 5620 SAM server station as the root user.

ii Open a console window on the 5620 SAM server station.

iii Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin directory.

iv Enter the following at the prompt:

\# **getDebugFiles.bash *directory*** ↵

where *directory* is the destination for the output files; this directory should have at least 4GB of free space

v Log in to the 5620 SAM database station as the root user.

vi Open a console window on the 5620 SAM database station.

vii Navigate to the 5620 SAM database binary directory, typically /opt/5620sam/samdb/install directory.

viii Enter the following at the prompt:

```
# getSAMDebugFiles.bash directory ↵
```

where *directory* is the destination for the output files; this directory should have at least 4GB of free space

ix Collect the following output files:

- the *server_hostname*.WsInfoFiles.tar.gz file, which contains basic 5620 SAM workstation information, including IP configuration details
- on the database station, the *server_hostname*.DBLogFiles.tar.gz file, which contains database logs and configuration details
- on the server station, the *server_hostname*.ServerLogFiles.tar.gz file, which contains server and JBoss logs and configuration details, including the output of the nms_status and nms_info nmsserver.bash utility.

x Send the files to Alcatel-Lucent technical support when requested.

9 Store the files in a secure location to ensure that the files are not overwritten. For example, if there are two 5620 SAM clients that experience problems, rename the files to identify each 5620 SAM client and to prevent the overwriting of one file with another of the same name.

Troubleshooting the managed network

3 — Troubleshooting using network alarms

3.1 Troubleshooting using network alarms

Incoming alarms from network components are displayed in the dynamic alarm list and are associated with objects that represent the affected network components. These alarms determine whether a problem exists.

Alarms raised against a network object are propagated to objects at higher levels in the managed object hierarchy. They are referred to as correlated alarms. To troubleshoot using network alarms, start with alarms on the lowest-level object in the managed object hierarchy. When these alarms are cleared, correlated alarms in the object hierarchy are cleared automatically.

A problem or alarm can be the result of one or more network problems. To identify the root cause of a problem, identify the root cause of individual alarms starting with alarms on the lowest-level managed object. If the affected object is not the cause of the alarm, the problem may be found on a related, supporting object below the lowest-level object in the alarm. After the problem is identified and fixed, the faulty network resource automatically clears the correlated alarms.

3.2 Workflow to troubleshoot using network alarms

1 You can:

a Use the dynamic alarm list.

i View and monitor alarms. See Procedure 3-1

ii Sort alarms in the dynamic alarm list according to time received. See Procedure 3-1.

b Use the navigation tree to view object alarms and aggregated alarms.

i View alarms from the navigation tree. See Procedure 3-2.

ii Navigate to aggregated or affect alarms from the properties form of the object. See Procedure 3-2.

2 Categorize alarms according to the managed object hierarchy and find the alarm with object type that is lowest in the network object hierarchy. See Procedure 3-3.

3 Acknowledge alarms on the affected object and on the related problems. See Procedure 3-4.

4 View detailed information about the alarm to determine the probable cause and, potentially, the root cause. See Procedure 3-5. The following sources of information are available:

i dynamic alarm list and Alarm Info forms

ii managed object hierarchy table

iii alarm description tables

5 View the affected object states information. See Procedure 3-5.

6 If there is an equipment down alarm, use the equipment view of the navigation tree for more information and check the physical connections to the port. See Procedure 3-8.

7 View related object information if the root cause is not found on the affected object. See Procedure 3-6.

8 Use the alarm description tables, alarm statistics, and the database of historical alarms, if required, to help interpret the data and troubleshoot network problems.

3.3 Troubleshooting using network alarms procedures

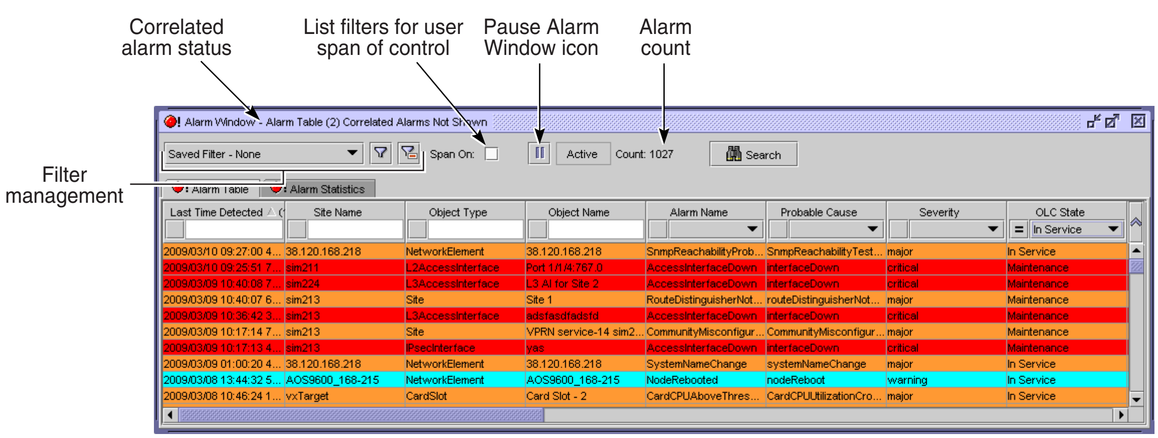
Use the following procedures to troubleshoot network problems using alarms.

Procedure 3-1 To view and sort alarms in the dynamic alarm list

Monitor the dynamic alarm list in the 5620 SAM alarm window and attempt to address alarms in the order that they are raised.

1 In the alarm window, click on the Alarm Table tab button to display the dynamic alarm list. Figure 3-1 shows the dynamic alarm list.

Figure 3-1 Dynamic alarm list



19623

2 Click on the First Time Detected column heading to sort the alarms in ascending order according to the first time the alarm was raised.

Multiple alarms received at approximately the same time indicate that the alarms may be correlated and may have a common root cause. Review the alarms in the order in which they are received. The alarm types, severity, and probable causes may provide the first indication of the root cause of the problem.

3 Before you start to deal with each alarm systematically, determine the total alarm count so that you can track your alarm-clearing progress.

Right-click on any column heading in the dynamic alarm list. The alarm count appears at the top of the contextual menu.

Procedure 3-2 To view object alarms and aggregated object alarms

You can use the navigation tree to view object alarm status, and aggregated alarm status for parent objects. See the *5620 SAM User Guide* for more information about the relationship between objects, related alarms, and aggregated alarms.

Consider the following:

- When an aggregated alarm is indicated, and no object alarm is seen for any child object, change the view of the equipment tree.
- An aggregated alarm may not appear in the selected view from the navigation tree. For example, with the Equipment drop-down menu selected, a critical alarm aggregated against the device object may appear. However, no object below the device object has a critical alarm. That is because the critical alarm is aggregated from the network view of the router. The alarm is based on the entire object, but the equipment view shows a subset of the entire object.

1 From the navigation tree, view alarms against objects. Alarms in circles are aggregated alarms. Alarms in squares are object alarms.

2 Right click on the object in the navigation tree and choose Properties from the contextual menu. The properties form appears.

3 Click on the Faults tab.

4 View object alarms from the Object Alarms tab button. View aggregated alarms against a parent object from the Aggregated Alarms tab button.

To view the object on which the aggregated alarm was raised:

i Choose an alarm from the aggregated alarms list.

ii Click on the View Alarm button. The Alarm Info form appears.

iii Click on the View Alarmed Object button. The properties form for the object appears.

Procedure 3-3 To categorize alarms by object hierarchy

1 In the alarm window, click on the Object Type column to sort the alarms alphabetically according to object type. If required, resize the column width to display the full text.

2 Scroll through the dynamic alarm list to locate the object type that is the lowest level in the network managed object hierarchy. Level 1 is the highest level, as listed in Table 3-1.

If two or more objects in the alarm are at the same level, choose the alarm with the earliest detected time. If two or more alarms at the same level are raised at the same time, use the alarm information provided to determine which alarm may be closer to the root cause of the problem and begin troubleshooting using this alarm.

Note — Alarm reporting latency can vary depending on network conditions. Therefore, the First Time Detected stamp is not a reliable indication of the exact time an event occurred and should be used only as an aid in troubleshooting.

Table 3-1 Hierarchy of 5620 SAM-managed objects

Level	Managed object	Alarm domain (domain descriptor)	For alarm information see
—	General network management or 5620 SAM objects	Accounting (accounting)	Table 3-2
		Alarm mapping (trapmapper)	Table 3-78
		Anti-spoofing (antispoof)	Table 3-4
		Application assurance (isa)	Table 3-28
		APS (aps)	Table 3-5
		Auto-config (autoconfig)	Table 3-7
		Database (db)	Table 3-13
		DHCP (dhcp)	Table 3-14
		File policy (file)	Table 3-21
		Generic object (generic)	Table 3-22
		LI (mirrorli)	Table 3-39
		Mediation (mediation)	Table 3-37
		MLD (mld)	Table 3-40
		MSDP (msdp)	Table 3-43
		NE security (sitesec)	Table 3-66
		Policy (policy)	Table 3-50
		PPP (ppp)	Table 3-51
		RADIUS accounting (radiusaccounting)	Table 3-53
		Residential subscriber (ressubscr)	Table 3-55
		Schedule (schedule)	Table 3-62
		Scheduler (vs)	Table 3-85
		Security (security)	Table 3-63
		Server (server)	Table 3-64
		SNMP (snmp)	Table 3-67
		Software (sw)	Table 3-74
		Subscriber identification (subscrident)	Table 3-71
		Template (template)	Table 3-77
		VRRP (vrrp)	Table 3-84

(1 of 3)

Level	Managed object	Alarm domain (domain descriptor)	For alarm information see
1	Network	CAC (cac)	Table 3-10
		CCAG (ccag)	Table 3-11
		Circuit emulation (circem)	Table 3-12
		IGH (igh)	Table 3-24
		IPsec (ipsec)	Table 3-27
		L2 (layer2)	Table 3-34
		L2 forwarding (l2fwd)	Table 3-30
		L3 forwarding (l3fwd)	Table 3-32
		LAG (lag)	Table 3-33
		Network (netw)	Table 3-46
		NE (rtr)	Table 3-59
		Multichassis (multichassis)	Table 3-44
		SRRP (srrp)	Table 3-70
2	Service	Aggregation scheduler (svq)	Table 3-72
		Epipe (epipe)	Table 3-15
		Ipipe (ipipe)	Table 3-26
		NAT (nat)	Table 3-45
		Resiliency (resiliency)	Table 3-54
		Service management (service)	Table 3-65
		Service mirror (mirror)	Table 3-38
		STM (sas)	Table 3-61
		VLANs (vlan)	Table 3-80
		VLL (vll)	Table 3-81
		VPLS (vpls)	Table 3-82
		VPRN (vprn)	Table 3-83
3	SDP binding	Service tunnel management (tunnelmgmt)	Table 3-79
4	Tunnel	Ethernet tunnel (ethernettunnel)	Table 3-19
		L2TP (l2tp)	Table 3-31
		MPLS (mpls)	Table 3-41
		Rules (rules)	Table 3-60
		Service tunnel (svt)	Table 3-73
5	LSP binding	MPLS (mpls)	Table 3-41
6	LSP		
7	Session	RSVP (rsvp)	Table 3-58
8	LDP interface or targeted peer	LDP (ldp)	Table 3-35

(2 of 3)

Level	Managed object	Alarm domain (domain descriptor)	For alarm information see
9	Network interface	BGP (bgp)	Table 3-8
		IGMP (igmp)	Table 3-25
		IS-IS (isis)	Table 3-29
		OSPF (ospf)	Table 3-48
		PIM (pim)	Table 3-49
		RIP (rip)	Table 3-56
10	Physical equipment	Equipment (equipment)	Table 3-16
		Ethernet equipment (ethernetequipment)	Table 3-17
		Ethernet OAM (ethernetoam)	Table 3-18
		Generic Network Element (genericne)	Table 3-23
		LPS (lps)	Table 3-36
		MPR (mpr)	Table 3-42
		RMON (rmon)	Table 3-57
		Wireless (radioequipment)	Table 3-52
11	SONET / SDH bundle	Bundle (bundle)	Table 3-9
	SONET	SONET (sonet)	Table 3-68
	SONET port/channel	SONET equipment (sonetequipment)	Table 3-69
12	DS1 / E1 channel	TDM equipment (tdmequipment)	Table 3-76

(3 of 3)

3 If you need more information about an alarm, find the alarm domain in the dynamic alarm list and see the appropriate table in section 3.5.

Procedure 3-4 To acknowledge alarms

When you select an alarm to investigate the root cause, you should acknowledge the alarm and its related problems to indicate that the problem is under investigation. This ensures that duplicate resources are not applied to the same problem.

1 To acknowledge the selected alarm

i Right-click on the selected alarm in the dynamic alarm list and choose Acknowledge Alarm(s) from the contextual menu. The Alarm Acknowledgement form opens.

If required, add text in the Acknowledgement Text box.

ii Select the Acknowledgement check box and click on the OK button. A command confirmation appears.

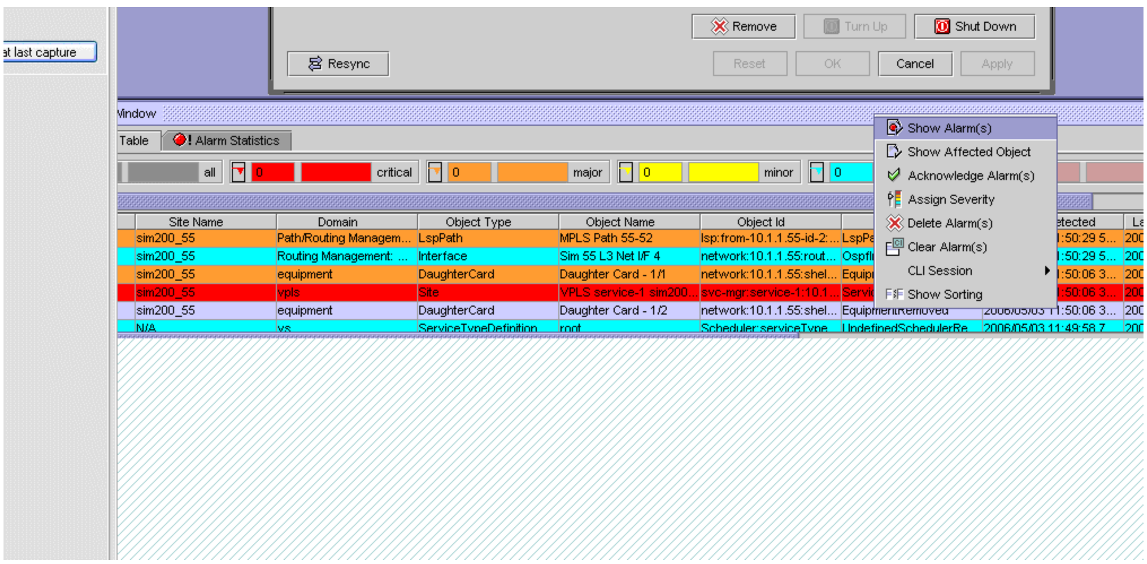
iii Click on the OK button to continue. A check mark appears for the selected alarm under the Ack. column in the dynamic alarm list.

2 To acknowledge multiple, correlated alarms

i Choose the selected alarm in the dynamic alarm list and choose Show Affected Object from the contextual menu. The properties form opens.

ii Click on the Faults tab button, then click on the Alarms on Related Objects or Affected Objects tab button to display the alarms related to the affected object, as shown in Figure 3-2.

Figure 3-2 Acknowledge related or affected problems



iii Choose all the alarms listed.

iv Right-click on the alarm list, then choose Acknowledge Alarm(s) from the contextual menu. The Alarm Acknowledgement form opens and lists all of the selected alarms. If required, add text in the Acknowledgement Text box.

v Click on the OK button. A command confirmation appears.

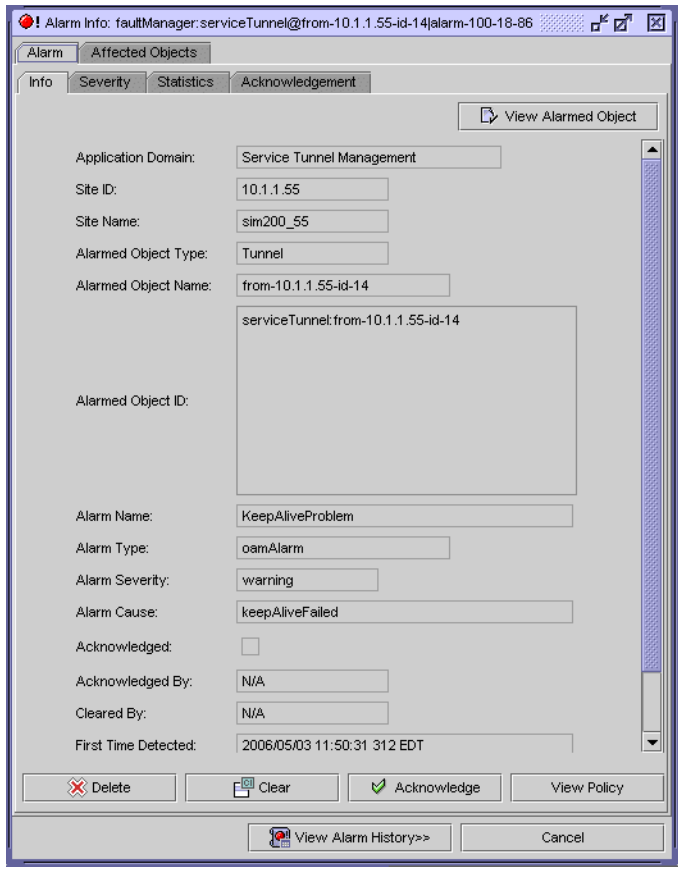
vi Click on the OK button to continue. A check mark appears for each of the selected alarms under the Ack. column in the dynamic alarm list.

Procedure 3-5 To determine probable cause and root cause using alarm and affected object information

Alarms are raised against managed objects. Objects with alarms are called affected objects.

1 Double-click on the selected alarm in the dynamic alarm list. The Alarm Info form opens as shown in the example in Figure 3-3.

Figure 3-3 Alarm Info form



The alarm cause indicates the probable cause, which can result from a problem on a related object lower in the hierarchy, even though no alarms are reported against it. However, the problem may be caused by the state conditions of the affected object itself.

2 To view the affected object states, click on the Affected Objects tab button, select an object and click on the View Object button.

a If the Administrative State is Up and the Operational State is Down, there are two possibilities:

- The affected object is the root cause of the problem. The alarm probable cause is the root cause. See section 3.5 for additional information about the alarm, which may help to correct the problem. When the problem is fixed, all correlated alarms are cleared. See section 3.4 for a sample equipment problem.

- The affected object is not the root cause of the problem. The alarm probable cause does not provide the root cause of the problem. The root cause is with a related, supporting object that is lower in the managed object hierarchy. Perform Procedure 3-6 to review related object information.

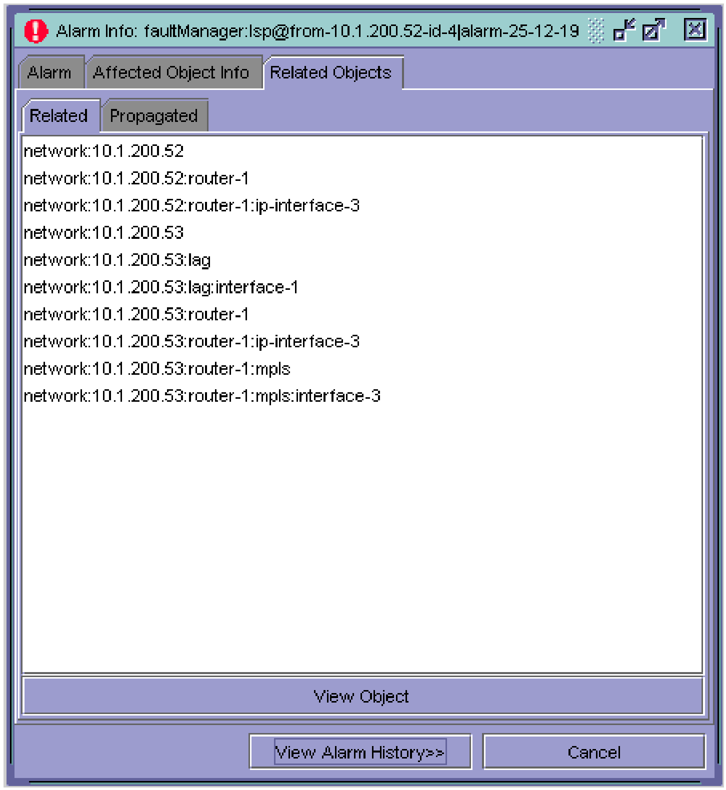
b If the Administrative State is Up and the Operational State is not Up or Down but states a specific problem such as Not Ready or MTU Mismatch, this is the root cause of the alarm. Correct the specified problem and all correlated alarms should clear. See section 3.4 for a sample configuration problem. If alarms still exist, perform Procedure 3-6.

c If the object Administrative State is Down, it is not the root cause of the alarm on the object; however, it may cause alarms higher in the network object hierarchy. Change the Administrative State to Up. See section 3.4 for a sample underlying port state problem. This does not clear the alarm on the affected object that you are investigating. Perform Procedure 3-6 to review related object information.

Procedure 3-6 To determine root cause using related objects

1 From the Alarm Info form for the affected object (see Procedure 3-5), click on the Affected Objects tab button. Figure 3-4 shows the related objects from the Related tab.

Figure 3-4 Related Objects



The Related tab button identifies the managed objects that are related to the object in the alarm and provides useful information for root cause analysis.

Select an object and click on the View Object button. Click on the Faults tab button, then click on the Alarms on Related Objects or Affected Objects tab button. This information shows aggregated or propagated alarm information. This information is not useful for root cause analysis but is helpful in identifying other affected objects.

2 Find the object type that is lowest in the network object hierarchy. See the object hierarchy in Table 3-1.

Through this process, you should find the lowest level managed object related to the object in the alarm.

3 Check the States information. This information should point to the root cause of the alarm. The problem should be found on the related, supporting object below the lowest level object in the alarm.

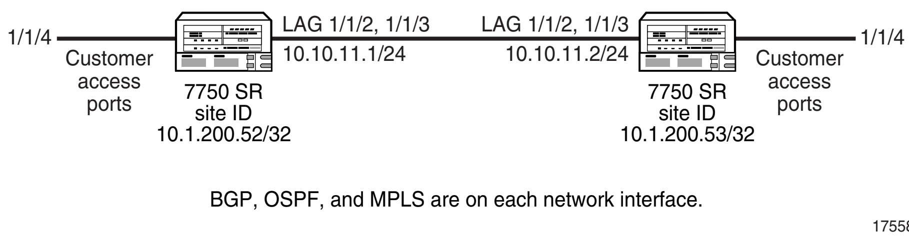
If required, check the Administrative State of the supporting port objects. A port with Administrative State Down does not generate alarms on the port, card, shelf, LAG, protocols, or sessions, but generates network path and service alarms. If the Administrative State is Down, change it to Up.

After the problem is fixed, the correlated alarms should automatically clear.

3.4 Sample problems

Figure 3-5 shows a two-node sample network configured with a VPLS that was used to create problems and generate alarms. This configuration generates the maximum number of alarms per problem type because alternate network paths are not available for self-healing.

Figure 3-5 Sample network



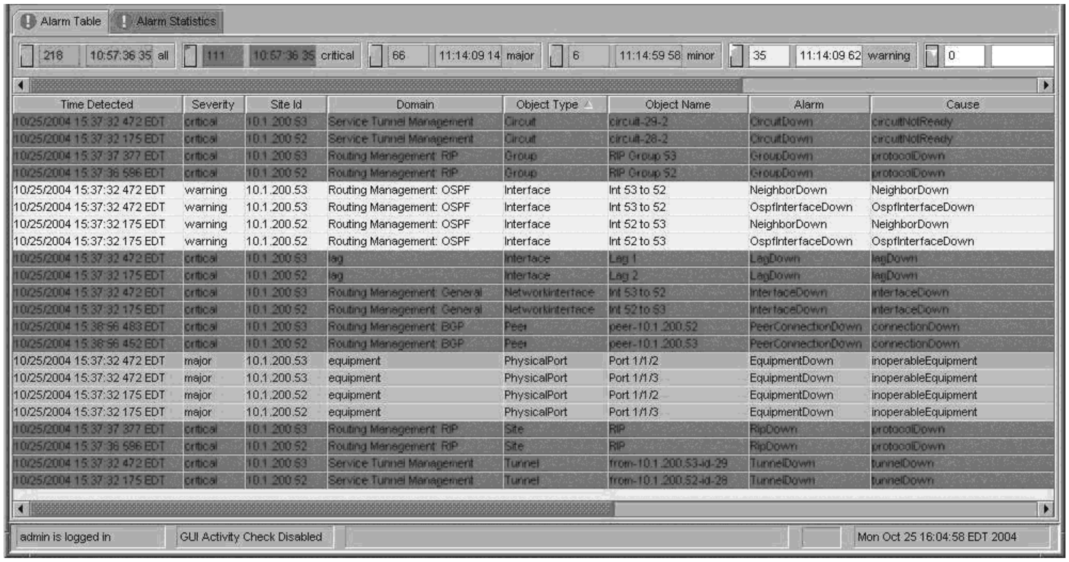
The dynamic alarm list is used to troubleshoot the following types of problems that are created.

- physical port problem that causes an Equipment Down alarm
- underlying port state problem that causes a number of related alarms at the LSP level
- configuration problem that causes a Frame Size Problem alarm

Troubleshooting a service equipment problem

A problem in the sample network produces the list of alarms shown in Figure 3-6.

Figure 3-6 Alarm list 1



The following procedure describes how to troubleshoot the problem.

Procedure 3-7 To troubleshoot a service equipment problem

1. Review the alarms in the order that they are raised. When the First Time Detected column or Last Time Detected column shows that the alarms are raised at approximately the same time, it is a good indication that these alarms may be correlated.

2. Determine the total alarm count to track the alarm-clearing progress. Right-click on any column heading in the dynamic alarm list. The contextual menu displays the alarm count.

3. Click on the Object Type column to sort the alarms alphabetically according to object type.

4. Scroll through the dynamic alarm list and find the object type that is lowest in the network object hierarchy, as listed in Table 3-1.

   In this example, the lowest-level object type in the alarm list is Physical Port in the equipment domain. There are four physical port objects in the alarm. Each alarm has the same severity level.

5. Choose one of the physical-port alarms and acknowledge the alarm.

   In this example, the alarm to investigate is one of the first two detected Physical Port alarms: Port 1/1/2 on Site ID 10.1.200.52.

6. Select the alarms related to this affected object and acknowledge the alarms.

7. View alarm information for the affected object. Double-click on the alarm in the list to view the information in the Alarm Info form.

8 Review the information about the alarm. In this example,

- The Equipment Down alarm is a Physical Port alarm in the Equipment domain.
- The device at Site ID 10.1.200.52. raised the alarm on object Port 1/1/2.
- The alarm cause is inoperable equipment.

9 Check the port states. Click on the Affected Objects tab button, then click on the View Object button to view state and other information about the object in the alarm.

In this case, the Administrative State is Up and the Operational State is Down, which results in an alarm. The Operational state cannot be modified manually.

10 The root cause is indicated by the probable cause of alarm on the affected object: physical Port 1/1/2 at site ID 10.1.200.52 is inoperable.

The dynamic alarm list also indicates that a second port on site 10.1.200.52, Port 1/1/3, is down. This port forms LAG 2 with port 1/1/2 and LAG 2 is down.

11 For equipment alarms, use the navigation tree view to identify the extent of the problem. Locate ports 1/1/2 and 1/1/3 under the Shelf object that supports LAG 2 at Site 10.1.200.52. The state for each port is operationally down. The tree view displays the aggregated alarms on objects up to the Router level.

A related LAG, LAG 1, is down but the alarms on LAG 2 ports were detected first.

Procedure 3-8 To clear alarms related to an equipment problem

This procedure describes how to clear the 22 alarms from the sample problem in this section. The troubleshooting process determined that two physical ports in LAG 2 at Site 10.1.200.52. are operationally down.

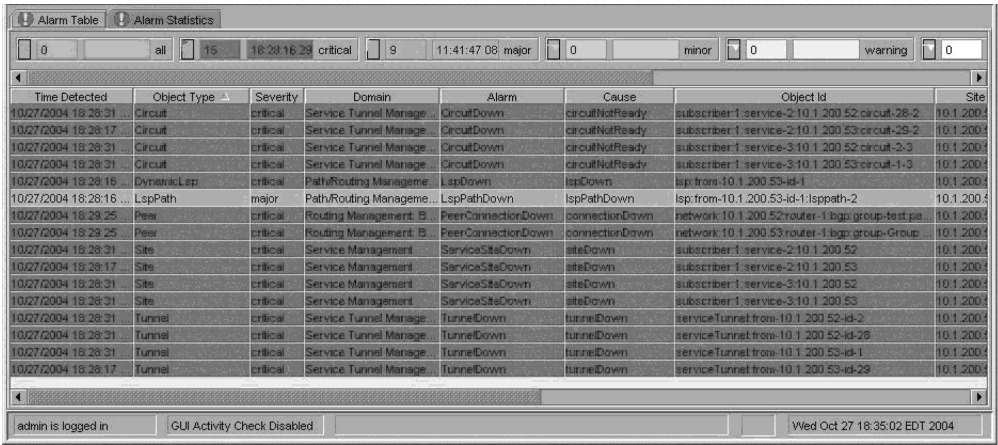
1 Check the physical connection to the port. The physical inspection shows that the two port connections supporting LAG 2 at Site 10.1.200.52. are not properly seated.

2 Seat the port connections. The 22 alarms, including the second two physical port Equipment Down alarms on LAG 1, automatically clear.

Troubleshooting an underlying port state problem

An underlying port state problem in the sample network produces the list of alarms shown in Figure 3-7.

Figure 3-7 Alarm list 2



The following procedure describes how to troubleshoot the problem.

Procedure 3-9 To troubleshoot an underlying port state problem

1 The First Time Detected column shows that 16 alarms are raised at approximately the same time, which is a good indication that these alarms may be correlated.

Note — The list contains an Lsp Down alarm and an Lsp Path Down alarm. Approximately one half hour later, a second Lsp Down alarm and a second Lsp Path Down alarm were raised for a total of 18 alarms.

2 Click on the Object Type column to sort the alarms alphabetically according to object type.

3 Scroll through the dynamic alarm list and find the object type that is lowest in the network object hierarchy, as listed in Table 3-1.

In this example, the lowest-level object type in the alarm list is Lsp Path in the Path/Routing Management domain. There are two Lsp Path Down alarms. One was raised later than the other.

4 Choose the earlier Lsp Path alarm and acknowledge the alarm.

Note — Alarm reporting latency can vary depending on network conditions. Therefore, the First Time Detected stamp is not a reliable indication of the exact time an event occurred and should be used only as an aid in troubleshooting.

5 Choose the alarms related to this affected object and acknowledge those alarms. In this case, the only alarm listed under Related Problems is the dynamic Lsp Down alarm.

6 View alarm information for the affected object. Double-click on the alarm in the list to view the information in the Alarm Info form.

7 Review the information about the alarm.

- Lsp Down is a path alarm on MPLS path 53 to 52.
- The affected object name and site name indicate that the alarm arose on the LSP path from device/site 53 to site 52.
- The Site information identifies the site that raised the alarm. The root cause is related to the device with Site Id 10.1.200.53.

8 Click on the View Alarmed Object button.

9 Click on the Faults tab button.

10 On the Alarm Info form, click on the Affected Object tab button and then click on the View Object button to view state and other information about the object in the alarm.

In this case, the Administrative State is Up and the Operational State is Down, which results in an alarm. The Operational State cannot be modified manually.

11 Check alarm description Table 3-41 for additional information, which in this case, indicates that the root cause may be a lower object in the managed object hierarchy.

12 View the details from the Related tab button on the Alarm Info form to display the managed objects related to the object in alarm.

13 Find the object type that is lowest in the network object hierarchy, as listed in Table 3-1. The lowest level object is a LAG.

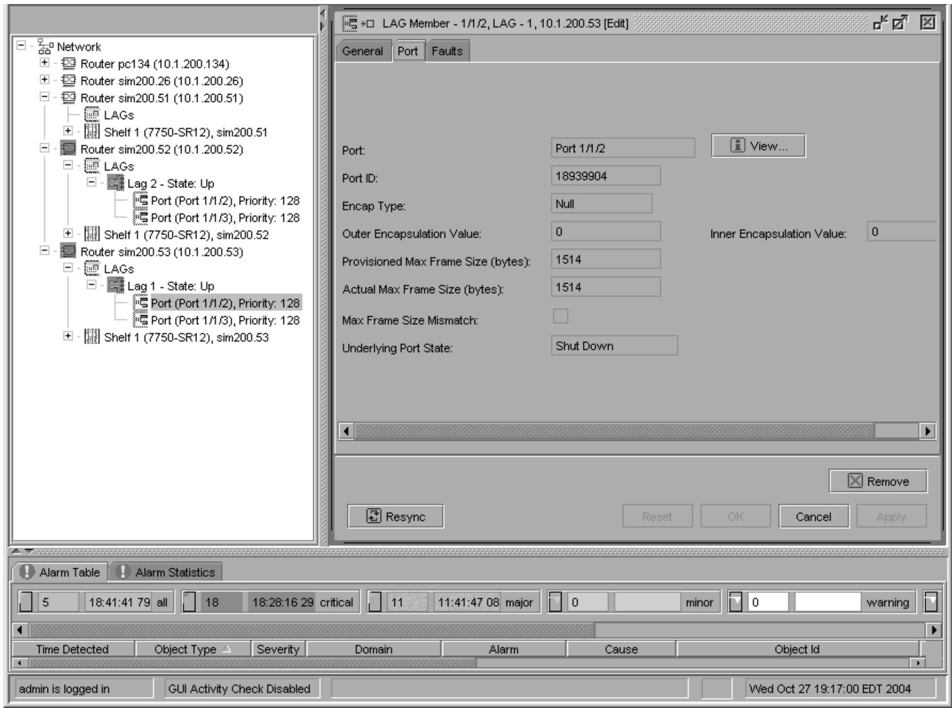
14 Open the equipment view of the navigation tree. It indicates that there are alarms related to both existing LAGs (Site Id 10.1.200.52 and Site Id 10.1.200.53). However, there is no LAG alarm in the dynamic alarm list and the LAG State is Up.

15 Check states of related, supporting objects for the lowest-level object in the alarm. Underlying port states may propagate alarms higher up the managed object hierarchy without causing alarms on ports, LAGs, interfaces, protocols, and sessions.

i In the equipment view of the navigation tree, choose a port under the LAG on Router 53 (Site 10.1.200.53) and choose Properties from the contextual menu. The LAG member properties form opens.

ii Click on the Port tab button to view the underlying port state of the LAG member, as shown in Figure 3-8. The LAG Member 1/1/2 properties form shows the Underlying Port State: Shut Down.

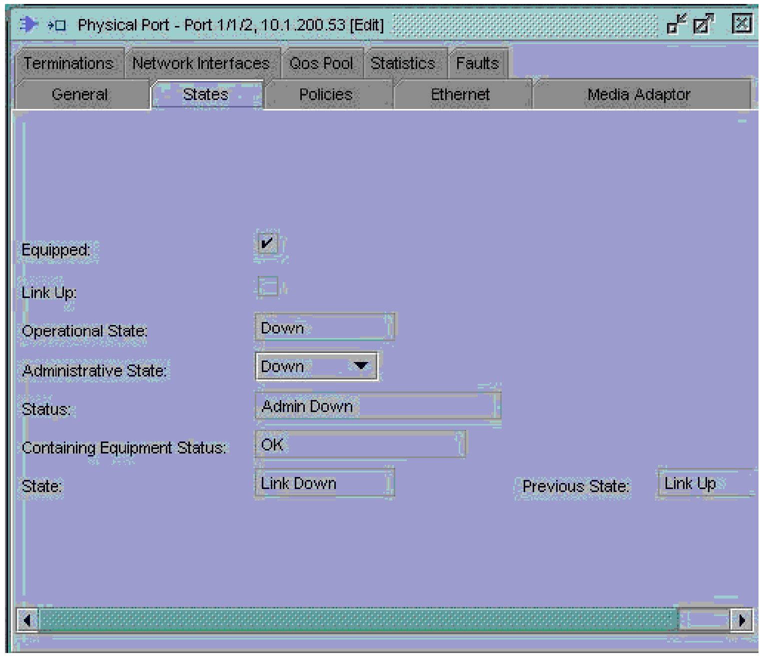
Figure 3-8 LAG member underlying port state in Properties form



iii Repeat step 15 ii for the second port. The LAG Member 1/1/3 properties form shows the State: Up.

16 In the equipment view of the navigation tree, choose port 1/1/2 under the Shelf object that supports LAG 1 (Site 10.1.200.53), and choose Properties from the contextual menu. The properties form opens, as shown in Figure 3-9.

Figure 3-9 Physical port states in Properties form



The form includes the following port information:

- Status is Admin Down.
- Operational State is Down
- Administrative State is Down
- Equipment Status is OK
- State: Link Down

There are no physical port equipment alarms. However, the port Status is Admin Down. This indicates that the root problem is the port Administrative state. Perform procedure 3-10 to clear alarms related to an underlying port state problems.

Procedure 3-10 To clear alarms related to an underlying port state problem

This procedure describes how to clear the 16 alarms from the sample problem described in this section. The troubleshooting process determined that a port, which supports LAG 1 at Site 10.1.200.53, is Down.

1. In the equipment view of the navigation tree, locate port 1/1/2 under the Shelf object supporting LAG 1 at Site 10.1.200.53. The State is Admin Down.

2. Choose the port and choose Turn Up from the contextual menu. Of the 18 alarms, 16 automatically clear. The remaining two alarms are Session alarms.

3 Choose one of the remaining alarms in the dynamic alarm list and choose Show Affected Object from the contextual menu. The affected object properties form opens.

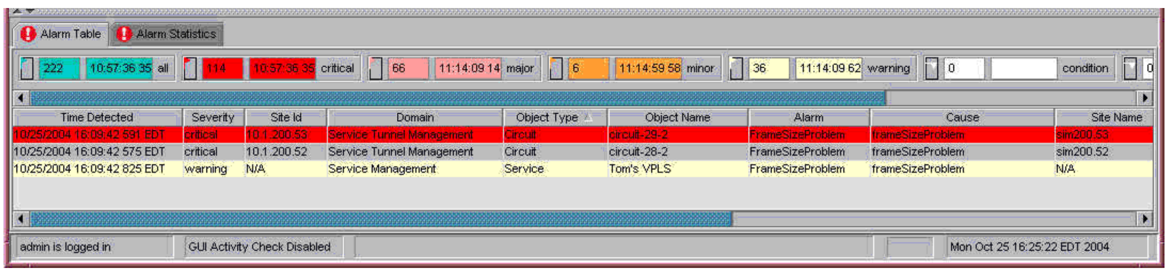
4 Click on the Resync button. An Object Deleted notification appears and the alarm clears automatically.

5 Repeat Steps 3 and 4 for the remaining alarm.

Troubleshooting a service configuration problem

A service configuration problem in the sample network produced the list of alarms shown in Figure 3-10.

Figure 3-10 Alarm list 3



The following procedure describes how to troubleshoot the problem.

Procedure 3-11 To troubleshoot a service configuration problem

1 Review the alarms in the order that they were raised. The First Time Detected column shows that three alarms were raised at the same time, which is a good indication that these may be correlated.

2 Find the object in the Object Type column that is lowest in the network object hierarchy as shown in Table 3-1. SDP binding is the lowest object. There are two SDP binding alarms on 28-2.

3 Choose one of the two SDP binding alarms and acknowledge the alarm. In this example, the selected alarm is SDP binding alarm (formerly CircuitAlarm): Site ID 10.1.200.53.

4 Select the alarms related to this affected object and acknowledge those alarms as described in Procedure 3-4.

5 Double-click on the alarm in the list to view information for the affected object in the Alarm Info form. Review the information about the alarm.

- Affected object is SDP binding (formerly known as circuit).
- Alarm type is configuration alarm.
- Probable cause is frame size problem.
- Domain is Service Tunnel Management.

6 Click on the Affected Objects tab button, then click on the View Object button to determine the SDP binding states.

- Administrative State is Up.
- Operational State is MTU Mismatch.

MTU Mismatch is the root cause of the Frame Size Problem alarm. You do not need to investigate the related objects.

7 Click on the Frame Size tab button on the SDP binding object form to find more information about the problem.

- The Max Frame Size Mismatch box is selected. The Max. Frame Size box shows a value greater than the value in the Actual Tunnel Max Frame Size box.
- The maximum frame size configured exceeds the maximum frame size supported for the service ingress and service egress termination points, which are also called the MTU.

8 Check Table 3-73 for additional information about the Frame Size Problem alarm.

Perform procedure 3-12 to clear the Frame Size Problem alarm.

Procedure 3-12 To clear a Frame Size Problem (MTU Mismatch) alarm

This procedure describes how to clear the SDP binding Frame Size Problem alarm described in this section.

1 Choose Manage→Services from the 5620 SAM main menu.

2 Configure the list filter criteria and click on the Search button. A list of services appears at the bottom of the Browse Services form.

3 Choose the service identified by the Alarmed Object Id in the Alarm Info form for the alarm that you are trying to clear.

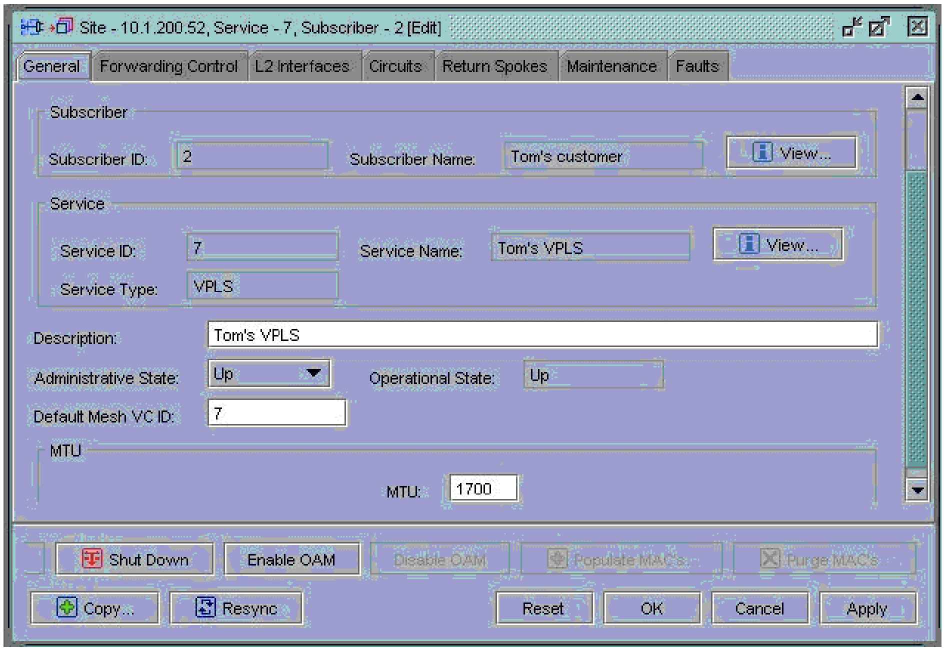
4 Click on the Properties button. The Service form opens.

5 Click on the Sites tab button. The list of available sites for the service appears.

6 Choose the site identified by the Site Id in the Alarm Info form for the alarm that you are trying to clear.

7 Click on the Properties button. The Site form opens as shown in Figure 3-11.

Figure 3-11 Site form

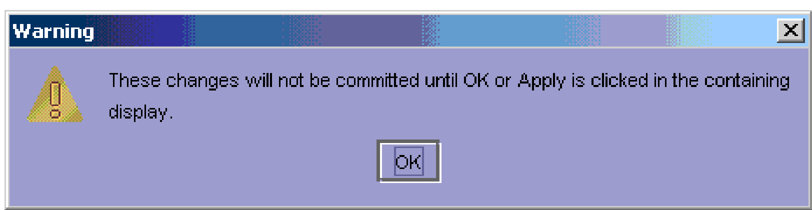


The MTU parameter indicates that the SDP binding maximum frame size is greater than the actual tunnel frame size of 1492 octets that supports the SDP binding.

8 Change the MTU to a value less than 1492, for example, 1000.

9 Click on the Apply button. A warning message appears, as shown in Figure 3-12. It warns you that changes to this Site form are not applied to the service unless you click on the OK or Apply button in the Service form.

Figure 3-12 Warning to apply changes to all objects



10 Click on the OK button. The Services form appears.

11 Click the Apply button. The warning message in Figure 3-12 again appears.

12 Click on the Apply button. The MTU configuration change is applied to customer, service, and site objects. The SDP binding and related service alarms clear automatically.

3.5 Alarm description tables

The following tables describe the alarms that the 5620 SAM can raise. The tables are in alphabetical order by domain, and the alarms within each table are in alphabetical order. A Type or Probable cause value includes a numeric identifier.

Note 1 — This guide does not include alarm information for the following domains:

- activation
- lte
- ltemme
- lteservice
- monpath
- topology

For activation, lte, ltemme, and lteservice alarm information, see the *5620 SAM LTE Alarm Reference*.

For monpath and topology alarm information, see the *5650 CPAM User Guide*.

Note 2 — This guide does not include information for alarms in the security domain that have a Type value of cpamLicensingAlarmType. For information about these alarms, see the *5650 CPAM User Guide*.

Table 3-2 Domain: accounting

Alarm	Attributes	Description
Name: AccountingPolicyDown (538) Type: AccountingPolicy (54) Probable cause: accountingPolicyDown (414)	Severity: Critical Object Type (class): Policy Domain: accounting Implicitly cleared (self-clearing): Yes	The alarm is raised when an accounting policy goes operationally Down after a file creation failure at the specified admin and backup locations.

Table 3-3 Domain: aclfilter

Alarm	Attributes	Description
Name: CreditControlInsertedFltrEntryDropped (1150) Type: configurationAlarm (11) Probable cause: FilterEntryDropped (856)	Severity: Warning Object Type (class): FilterDefinition Domain: aclfilter Implicitly cleared (self-clearing): No	The alarm is raised when a request to insert a filter entry was not successful in Credit Control range.
Name: CreditControlInsertSpaceThresholdAlarm (1149) Type: configurationAlarm (11) Probable cause: UtilizationExceedConfiguredLimit (855)	Severity: Major Object Type (class): FilterDefinition Domain: aclfilter Implicitly cleared (self-clearing): Yes	The alarm is generated when the utilization of a filter entry range that was reserved for filter entry insertionincreases to the configured high watermark for Credit Control application insert range.

(1 of 2)

Alarm	Attributes	Description
Name: RadiusInsertedFltrEntryDropped (1152) Type: configurationAlarm (11) Probable cause: FilterEntryDropped (856)	Severity: Warning Object Type (class): FilterDefinition Domain: aclfilter Implicitly cleared (self-clearing): No	The alarm is raised when a request to insert a filter entry was not successful in Radius range.
Name: RadiusInsertSpaceThresholdAlarm (1151) Type: configurationAlarm (11) Probable cause: UtilizationExceedConfiguredLimit (855)	Severity: Major Object Type (class): FilterDefinition Domain: aclfilter Implicitly cleared (self-clearing): Yes	The alarm is generated when the utilization of a filter entry range that was reserved for filter entry insertionincreases to the configured high watermark for Radius application insert range.

(2 of 2)

Table 3-4 Domain: antispoof

Alarm	Attributes	Description
Name: SapStaticHostDynamicMacConflict (313) Type: configurationAlarm (11) Probable cause: LearnedDynamicMacAlreadyLearned (243)	Severity: Minor Object Type (class): AntiSpoofingStaticHosts Domain: antispoof Implicitly cleared (self-clearing): No	The alarm is raised when an NE tries to learn a dynamic MAC address from an IP-only static host.

Table 3-5 Domain: aps

Alarm	Attributes	Description
Name: IncorrectNeighborConfig (609) Type: configurationAlarm (11) Probable cause: incorrectNeighborConfig (452)	Severity: Major Object Type (class): ApsGroup Domain: aps Implicitly cleared (self-clearing): Yes	The alarm is raised when the peer does not exist or the neighbor address does not point to a network interface on the NE that contains the peer object.

Table 3-6 Domain: atm

Alarm	Attributes	Description
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm (18) Probable cause: networkDegradation (204)	Severity: Major Object Type (class): PvcConnection Domain: atm Implicitly cleared (self-clearing): Yes	The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.

Table 3-7 Domain: autoconfig

Alarm	Attributes	Description
Name: DeployProfileFailed (610) Type: configurationAlarm (11) Probable cause: DeployProfileFailed (453)	Severity: Major Object Type (class): AutoProvisioning Domain: autoconfig Implicitly cleared (self-clearing): No	The alarm is raised when the deployment of a script to a 7705 SAR fails.

Table 3-8 Domain: bgp

Alarm	Attributes	Description
Name: BgpDown (6) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): Site Domain: bgp Implicitly cleared (self-clearing): Yes	The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.
Name: HoldTimeInconsistent (810) Type: ProtocolAlarm (1) Probable cause: holdTimeInconsistent (575)	Severity: Major Object Type (class): Peer Domain: bgp Implicitly cleared (self-clearing): No	The alarm is raised when a BGP site tries to establish a peering using a hold time that is less than the configured strict hold time. The peering is rejected as a result.
Name: PeerConnectionDown (2) Type: ProtocolAlarm (1) Probable cause: connectionDown (2)	Severity: Critical Object Type (class): Peer Domain: bgp Implicitly cleared (self-clearing): Yes	The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.
Name: PeerDown (1) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): Peer Domain: bgp Implicitly cleared (self-clearing): Yes	The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.
Name: PeerGroupDown (5) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): PeerGroup Domain: bgp Implicitly cleared (self-clearing): Yes	The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.
Name: PrefixLimitExceeded (4) Type: ProtocolAlarm (1) Probable cause: prefixLimitExceeded (4)	Severity: Critical Object Type (class): Peer Domain: bgp Implicitly cleared (self-clearing): No	The alarm is raised when a BGP instance learns the maximum number of peer routes.
Name: PrefixLimitNearing (3) Type: ProtocolAlarm (1) Probable cause: prefixLimitNearing (3)	Severity: Major Object Type (class): Peer Domain: bgp Implicitly cleared (self-clearing): No	The alarm is raised when a BGP instance learns 90 percent of the maximum number of peer routes.

Table 3-9 Domain: bundle

Alarm	Attributes	Description
Name: AsymmetricalConfig (295) Type: configurationAlarm (11) Probable cause: asymmetricalConfig (226)	Severity: Major Object Type (class): MultiChassisApsInterface Domain: bundle Implicitly cleared (self-clearing): Yes	The alarm is raised when the bundles in an APS group do not have matching configurations.
Name: BundleDown (152) Type: equipmentAlarm (3) Probable cause: bundleDown (128)	Severity: Critical Object Type (class): Interface Domain: bundle Implicitly cleared (self-clearing): Yes	The alarm is raised when the bundle Administrative State is Up and the Operational State is Down.
Name: IncompleteConfig (294) Type: configurationAlarm (11) Probable cause: incompleteConfig (225)	Severity: Major Object Type (class): MultiChassisApsInterface Domain: bundle Implicitly cleared (self-clearing): Yes	The alarm is raised when there are not exactly two APS bundles in an APS group.
Name: TrailSignalFail (798) Type: communicationsAlarm (4) Probable cause: trailSignalFailure (565)	Severity: Major Object Type (class): Interface Domain: bundle Implicitly cleared (self-clearing): Yes	The alarm is raised when a a local or remote failure in an IMA group generates a Trail Signal Fail message.

Table 3-10 Domain: cac

Alarm	Attributes	Description
Name: BWUtilizationExceeded (811) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Major Object Type (class): AbstractPhysicalLinkBandwidth Domain: cac Implicitly cleared (self-clearing): Yes	The alarm is raised when the per-CoS or overall bandwidth utilization exceeds the configured threshold.

Table 3-11 Domain: ccag

Alarm	Attributes	Description
Name: CcagDown (210) Type: equipmentAlarm (3) Probable cause: CcagDown (163)	Severity: Major Object Type (class): CrossConnectAggregationGroup Domain: ccag Implicitly cleared (self-clearing): Yes	The alarm is raised when the CCAG Administrative State is Up and the Operational State is Down.

Table 3-12 Domain: circem

Alarm	Attributes	Description
Name: BatmPWVcCurrentFarEndFC (324) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): Interface Domain: circem Implicitly cleared (self-clearing): No	The alarm is raised when the current number of remote packet failures crosses the threshold.
Name: BatmPWVcCurrentJtrBfrOverruns (318) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): Interface Domain: circem Implicitly cleared (self-clearing): No	The alarm is raised when the current number of out-of-range packets that could not be re-ordered or fit in the jitter buffer crosses the threshold.The packet range is indicated by the TDM header sequence numbers.
Name: BatmPWVcCurrentJtrBfrUnderruns (316) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): Interface Domain: circem Implicitly cleared (self-clearing): No	The alarm is raised when the current number of jitter buffer underruns crosses the threshold.
Name: BatmPWVcCurrentMalformedPkt (320) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): Interface Domain: circem Implicitly cleared (self-clearing): No	The alarm is raised when the current number of packets in the Unexpected Size or Bad Headers stack crosses the threshold.
Name: BatmPWVcCurrentNearEndFC (322) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): Interface Domain: circem Implicitly cleared (self-clearing): No	The alarm is raised when the current number of local packet failures crosses the threshold.
Name: BatmPWVcCurrentPktsOoseq (314) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): Interface Domain: circem Implicitly cleared (self-clearing): No	The alarm is raised when the current number of successfully re-ordered out-of-sequence packets crosses the threshold.The packet sequence is indicated by the TDM header sequence numbers.
Name: BatmPWVcFarEndFC (325) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): Interface Domain: circem Implicitly cleared (self-clearing): No	The alarm is raised when the total number of remote packet failures crosses the threshold.
Name: BatmPWVcJtrBfrOverruns (319) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): Interface Domain: circem Implicitly cleared (self-clearing): No	The alarm is raised when the total number of out-of-range packets that could not be re-ordered or fit in the jitter buffer crosses the threshold. The packet range is indicated by the TDM header sequence numbers.
Name: BatmPWVcJtrBfrUnderruns (317) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): Interface Domain: circem Implicitly cleared (self-clearing): No	The alarm is raised when the total number of jitter buffer underruns crosses the threshold.
Name: BatmPWVcMalformedPkt (321) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): Interface Domain: circem Implicitly cleared (self-clearing): No	The alarm is raised when the total number of packets in the Unexpected Size or Bad Headers stack crosses the threshold.

(1 of 2)

Alarm	Attributes	Description
Name: BatmPWVcNearEndFC (323) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): Interface Domain: circem Implicitly cleared (self-clearing): No	The alarm is raised when the total number of local packet failures crosses the threshold.
Name: BatmPWVcPktsOoseq (315) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): Interface Domain: circem Implicitly cleared (self-clearing): No	The alarm is raised when the total number of successfully re-ordered out-of-sequence packets crosses the threshold.The packet sequence is indicated by the TDM header sequence numbers.

(2 of 2)

Table 3-13 Domain: db

Alarm	Attributes	Description
Name: AllArchiveLogsDeleted (199) Type: databaseAlarm (29) Probable cause: archivedLogsIssue (154)	Severity: Warning Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM deletes all database archive logs because it requires more disk space.When database disk space is low, the 5620 SAM first deletes the archive logs that have been applied to the standby database and raises the OldArchiveLogsDeleted alarm. If deleting the applied archive logs does not free up sufficient disk space, the 5620 SAM deletes the remaining archive logs, which creates an archive log gap that requires a standby database reinstantiation to correct.The alarm is raised only in a redundant 5620 SAM system.
Name: ArchiveLogDiskSpaceBelowThreshold (197) Type: databaseAlarm (29) Probable cause: diskSpaceIssue (153)	Severity: Critical Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): No	The alarm is raised when the primary or standalone database archive log disk space threshold specified in the nms-server.xml file is reached.
Name: BackupDiskSpaceBelowThreshold (195) Type: databaseAlarm (29) Probable cause: diskSpaceIssue (153)	Severity: Critical Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): No	The alarm is raised when the primary or standalone database backup disk space threshold specified in the nms-server.xml file is reached.
Name: DatabaseArchivedLogNotApplied (205) Type: configurationAlarm (11) Probable cause: databaseArchivedLogNotApplied (159)	Severity: Warning Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when, during a database backup, the 5620 SAM determines that the archive logs are not being applied to the standby database, as indicated by the archive log gap. The archive log gap threshold is defined in the nms-server.xml file.The alarm is raised only in a redundant 5620 SAM system.

(1 of 5)

Alarm	Attributes	Description
Name: DatabaseBackupFailed (136) Type: configurationAlarm (11) Probable cause: databaseBackupFailure (109)	Severity: Major Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): No	The alarm is raised when the database backup files cannot be created because of, for example, a lack of disk space or insufficient file permissions.
Name: DatabaseBackupInvalidConfig (1117) Type: configurationAlarm (11) Probable cause: InvalidbBackupConfigration (829)	Severity: Major Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when the scheduled backup destination is empty.
Name: DatabaseBackupRsyncFailed (749) Type: databaseAlarm (29) Probable cause: databaseBackupFileRsyncFailed (525)	Severity: Warning Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): No	The alarm is raised when one or more database backup files cannot be copied to the standby database station.
Name: DatabaseRedundancyArchiveGap (611) Type: configurationAlarm (11) Probable cause: DatabaseRedundancyArchiveGap (454)	Severity: Major Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when the primary 5620 SAM main server detects an archive log gap. An archive log gap occurs when a number of archive logs cannot be applied to the standby database. The alarm may indicate that the primary database is out of archive log disk space, the standby database has been down for too long, or the standby database is not able to process the archive logs at the rate that the primary database sends them. The alarm clears after a standby database reinstantiation, which corrects the archive log gap.The alarm is raised only in a redundant 5620 SAM system.
Name: DatabaseRedundancyFailure (246) Type: configurationAlarm (11) Probable cause: DatabaseRedundancyFailure (184)	Severity: Major Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects a standby database problem, for example, the database is down or not in managed recovery mode. The alarm clears when the standby database is functional.The alarm is raised only in a redundant 5620 SAM system.
Name: DatabaseRedundancyOutOfSync (302) Type: configurationAlarm (11) Probable cause: DatabaseRedundancyOutOfSync (233)	Severity: Warning Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when the primary 5620 SAM server polls the primary and standby databases and detects a difference in the primary and standby database archive log sequence numbers that is greater than one. The alarm may indicate that the primary database is not sending archive logs to the standby quickly enough, or that the standby database is not able to process the archive logs at the rate that the primary sends them.The alarm is raised only in a redundant 5620 SAM system.

(2 of 5)

Alarm	Attributes	Description
Name: DatabaseRedundancyRealTimeApplyFailure (296) Type: configurationAlarm (11) Probable cause: DatabaseRedundancyRealTimeApplyFailure (227)	Severity: Warning Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when database redundancy falls out of real-time apply transfer mode, which means that the primary database transactions are not immediately replicated to the standby database. The alarm clears when the database is operating in real-time apply mode.
Name: DataFileDiskSpaceBelowThreshold (196) Type: databaseAlarm (29) Probable cause: diskSpaceIssue (153)	Severity: Critical Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when the primary or standalone database data file disk space threshold specified in the nms-server.xml file is reached.
Name: DatafileSizeAboveThreshold (750) Type: databaseAlarm (29) Probable cause: HighNumberOfRecords (526)	Severity: Critical Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): No	The alarm is raised when a tablespace data file size exceeds 85 percent of 32 Gbytes. This may indicate that the number of stored NE backups is too high.
Name: DBFailOver (201) Type: configurationAlarm (11) Probable cause: databasePrimaryDown (155)	Severity: Critical Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when a database failover occurs. A standby database reinstantiation is required. The alarm clears when the standby database is online.
Name: InstallDirectoryDiskSpaceBelowThreshold (612) Type: databaseAlarm (29) Probable cause: diskSpaceIssue (153)	Severity: Major Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when the primary or standalone database installation disk space threshold specified in the nms-server.xml file is reached.
Name: OldArchiveLogsDeleted (198) Type: databaseAlarm (29) Probable cause: archivedLogsIssue (154)	Severity: Warning Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM deletes the applied archive logs because database disk space is low. In a standalone deployment, the 5620 SAM deletes all archive logs. In a redundant deployment, the 5620 SAM deletes the applied archive logs, and can raise the alarm against the primary or standby database.
Name: OracleHomeDiskSpaceBelowThreshold (399) Type: databaseAlarm (29) Probable cause: diskSpaceIssue (153)	Severity: Major Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when the primary or standalone database Oracle disk space threshold specified in the nms-server.xml file is reached.
Name: PrimaryDatabaseDown (751) Type: databaseAlarm (29) Probable cause: primaryDatabaseDown (527)	Severity: Critical Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when the primary 5620 SAM database is down for at least one poll. The alarm is not persisted in the database or stored in the alarm history; when the database returns to service, the PrimaryDatabaseWasDown alarm is raised.

(3 of 5)

Alarm	Attributes	Description
Name: PrimaryDatabaseWasDown (254) Type: databaseAlarm (29) Probable cause: primaryDatabaseWasDown (193)	Severity: Warning Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): No	The alarm is raised when the primary database returns to service after being unavailable for at least one poll.
Name: ProxyDown (1959) Type: communicationsAlarm (4) Probable cause: systemFailed (144)	Severity: Major Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when proxy server communication fails.
Name: RealignmentOfDatabase (613) Type: configurationAlarm (11) Probable cause: databaseRealignment (455)	Severity: Warning Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): No	The alarm is raised when the primary 5620 SAM main server realigns itself with the preferred database by performing a database switchover to connect to the primary database.
Name: RealignmentOfDatabaseFailed (614) Type: configurationAlarm (11) Probable cause: databaseRealignmentFailed (456)	Severity: Critical Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): No	The alarm is raised when a database switchover to realign the primary main server and primary database fails. The primary main server is not connected to the preferred database.
Name: ReinstantiateStandbyDatabase (252) Type: configurationAlarm (11) Probable cause: reinstantiateStandbyDatabase (191)	Severity: Warning Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): No	The alarm is raised when a standby database reinstantiation occurs.
Name: ReinstantiateStandbyDatabaseFailed (253) Type: configurationAlarm (11) Probable cause: reinstantiateStandbyDatabaseFailed (192)	Severity: Critical Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): No	The alarm is raised when a standby database reinstantiation fails.
Name: RowThresholdConstraintViolated (286) Type: configurationAlarm (11) Probable cause: partialConstraintEnforcement (218)	Severity: Major Object Type (class): SizeConstraintPolicy Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of records in a database table exceeds the number specified in a size constraint policy.
Name: StagingDiskSpaceBelowThreshold (453) Type: databaseAlarm (29) Probable cause: diskSpaceIssue (153)	Severity: Major Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when the primary or standalone database staging disk space threshold specified in the nms-server.xml file is reached.
Name: StandbyDataFileDiskSpaceBelowThreshold (539) Type: databaseAlarm (29) Probable cause: diskSpaceIssue (153)	Severity: Critical Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when the standby data file disk space threshold specified in the nms-server.xml file is reached.

(4 of 5)

Alarm	Attributes	Description
Name: StandbyInstallDirectoryDiskSpaceBelowThreshold (615) Type: databaseAlarm (29) Probable cause: diskSpaceIssue (153)	Severity: Major Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when the standby database installation disk space threshold specified in the nms-server.xml file is reached.
Name: StandbyOracleHomeDiskSpaceBelowThreshold (540) Type: databaseAlarm (29) Probable cause: diskSpaceIssue (153)	Severity: Major Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when the standby database Oracle disk space threshold specified in the nms-server.xml file is reached.
Name: StandbyStagingDiskSpaceBelowThreshold (541) Type: databaseAlarm (29) Probable cause: diskSpaceIssue (153)	Severity: Major Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when the standby database staging disk space threshold specified in the nms-server.xml file is reached.
Name: SwitchOverDatabase (203) Type: configurationAlarm (11) Probable cause: switchOverDatabase (157)	Severity: Warning Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): No	The alarm is raised when a database switchover occurs.
Name: SwitchOverDatabaseFailed (204) Type: configurationAlarm (11) Probable cause: switchOverDatabaseFailed (158)	Severity: Critical Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): No	The alarm is raised when a database switchover fails.
Name: TableSpaceAboveThreshold (454) Type: databaseAlarm (29) Probable cause: HighStatisticsCollectionRate (349)	Severity: Critical Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): No	The alarm is raised when the database table space becomes too full, which may indicate that the performance statistics collection rate or the statistics retention time is too high.
Name: TwoPrimaryDatabase (202) Type: configurationAlarm (11) Probable cause: twoPrimaryDatabase (156)	Severity: Critical Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): Yes	The alarm is raised when the standby database initializes as a primary database because of a database failover. The alarm clears when the original primary database is operational as the new standby database.
Name: UnableDeleteArchivedLogs (200) Type: databaseAlarm (29) Probable cause: archivedLogsIssue (154)	Severity: Major Object Type (class): DatabaseManager Domain: db Implicitly cleared (self-clearing): No	The alarm is raised when database disk space is low and the 5620 SAM is unable to delete the archive logs.

(5 of 5)

Table 3-14 Domain: dhcp

Alarm	Attributes	Description
Name: FailoverUnavailable (1155) Type: configurationAlarm (11) Probable cause: failoverUnavailable (858)	Severity: Minor Object Type (class): LocalDhcpServerFailover Domain: dhcp Implicitly cleared (self-clearing): Yes	The alarm is raised when the Local DHCP Server Failover has a state other than Normal.
Name: FailoverUpdateFailed (1156) Type: configurationAlarm (11) Probable cause: updateFailed (859)	Severity: Warning Object Type (class): LocalDhcpServerFailover Domain: dhcp Implicitly cleared (self-clearing): No	The alarm is raised when the Local DHCP Server Failover update has failed.
Name: SubnetMinFreeExc (516) Type: configurationAlarm (11) Probable cause: actualFreeAddrBelowSubnetMin (391)	Severity: Warning Object Type (class): Subnet Domain: dhcp Implicitly cleared (self-clearing): No	The alarm is raised when the actual number of free addresses in a subnetfalls below the desired minimum number specified in the subnet configuration

Table 3-15 Domain: epipe

Alarm	Attributes	Description
Name: BWUtilizationExceededOnTunnel (812) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Major Object Type (class): Epipe Domain: epipe Implicitly cleared (self-clearing): Yes	The alarm is raised when the per-CoS or overall bandwidth utilization on a tunnel exceeds the configured threshold.
Name: ForceQTagForwardingMisconfiguration (813) Type: configurationAlarm (11) Probable cause: forceQTagForwardingInconsistent (576)	Severity: Warning Object Type (class): Epipe Domain: epipe Implicitly cleared (self-clearing): Yes	The alarm is raised when two I-sites in a service use different Force Q Tag Forwarding values.
Name: IsidMisconfiguration (592) Type: configurationAlarm (11) Probable cause: isidInconsistent (446)	Severity: Warning Object Type (class): Epipe Domain: epipe Implicitly cleared (self-clearing): Yes	The alarm is raised when Epipe service sites that are bound to a PBB backbone use different ISID values.

Table 3-16 Domain: equipment

Alarm	Attributes	Description
Name: Ais (736) Type: communicationsAlarm (4) Probable cause: ais (513)	Severity: Minor Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE reports an AIS condition on the Tx or Rx circuit of a PDH tributary.

(1 of 17)

Alarm	Attributes	Description
Name: AisRx (1157) Type: communicationsAlarm (4) Probable cause: aisRx (860)	Severity: Minor Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when there is a transmission alarm indication signal.
Name: AisTx (1158) Type: communicationsAlarm (4) Probable cause: aisTx (861)	Severity: Minor Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when there is a transmission alarm indication signal.
Name: AncillaryPathLimitReached (459) Type: resourceAlarm (28) Probable cause: resourceLimitReached (131)	Severity: Warning Object Type (class): DaughterCard Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the ancillary path bandwidth limit is reached.
Name: AtcaFanFailure (1124) Type: equipmentAlarm (3) Probable cause: fanFailure (116)	Severity: Critical Object Type (class): Fan Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the associated fan is not operationally Up.
Name: AtcaPowerSupplyFailure (1125) Type: equipmentAlarm (3) Probable cause: fanFailure (116)	Severity: Critical Object Type (class): PowerSupply Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the associated power supply is not operationally Up.
Name: AuxiliaryAlarm (1159) Type: dryContactAlarm (47) Probable cause: auxliaryAlarmTriggered (862)	Severity: Variable or indeterminate Object Type (class): AuxAlarmDefinition Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when an NE reports that a configured auxiliary alarmcondition has been triggered.
Name: BackgroundDiagnosticFault (467) Type: equipmentAlarm (3) Probable cause: backgroundDiagnosticFault (353)	Severity: Minor Object Type (class): ReplaceableUnit Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE detects a failure in a background diagnostic test suite.
Name: BatmDsx1CurrentCSSs (336) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the current number of far-end Controlled Slip Seconds crosses the threshold.
Name: BatmDsx1CurrentESs (330) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the current number of far-end Errored Seconds crosses the threshold.
Name: BatmDsx1CurrentLESs (326) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the current number of Line Errored Seconds crosses the threshold.
Name: BatmDsx1CurrentPVCs (328) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the current number of Path Coding Violations crosses the threshold.

(2 of 17)

Alarm	Attributes	Description
Name: BatmDsx1CurrentSEFSs (334) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the current number of far-end Severely Errored Framing Seconds crosses the threshold.
Name: BatmDsx1CurrentSESs (332) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the current number of far-end Severely Errored Seconds crosses the threshold.
Name: BatmDsx1CurrentUASs (338) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the current number of Unavailable Seconds crosses the threshold.
Name: BatmDsx1TotalCSSs (337) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the total number of far-end Controlled Slip Seconds crosses the threshold.
Name: BatmDsx1TotalESs (331) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the total number of far-end Errored Seconds crosses the threshold.
Name: BatmDsx1TotalLESs (327) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the total number of Line Errored Seconds crosses the threshold.
Name: BatmDsx1TotalPVCs (329) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the total number of Path Coding Violations crosses the threshold.
Name: BatmDsx1TotalSEFSs (335) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the total number of far-end Severely Errored Framing Seconds crosses the threshold.
Name: BatmDsx1TotalSESs (333) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the total number of far-end Severely Errored Seconds crosses the threshold.
Name: BatmDsx1TotalUASs (339) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the total number of Unavailable Seconds crosses the threshold.
Name: BatteryFail (616) Type: equipmentAlarm (3) Probable cause: batteryFail (457)	Severity: Warning Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the battery fails or is missing.

(3 of 17)

Alarm	Attributes	Description
Name: BootLoaderFirmwareMismatchAlarm (617) Type: firmwareAlarm (26) Probable cause: bootLoaderVersionMismatch (118)	Severity: Critical Object Type (class): ControlProcessor Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when there is a mismatch between the firmware version and the software image on an NE. The alarm information includes the discovered and expected version identifiers.
Name: BrokenLoop (469) Type: configurationAlarm (11) Probable cause: stackNotInLoop (355)	Severity: Major Object Type (class): StackConfiguration Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the loop-detection stack detects a loop condition, or when the stack contains an unexpected element.
Name: CableLOS (678) Type: communicationsAlarm (4) Probable cause: cableLOS (493)	Severity: Major Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an MSS detects a cable LOS event.
Name: CardCPUAboveThreshold (618) Type: configurationAlarm (11) Probable cause: CardCPUUtilizationCrossedAboveThreshold (458)	Severity: Major Object Type (class): CardSlot Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the card CPU usage exceeds the threshold value.
Name: CardMemoryAboveThreshold (619) Type: configurationAlarm (11) Probable cause: CardMemoryUtilizationCrossedAboveThresh old (459)	Severity: Major Object Type (class): CardSlot Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the card memory usage exceeds the threshold value.
Name: CardMismatch (1160) Type: equipmentAlarm (3) Probable cause: CardMismatch (863)	Severity: Major Object Type (class): CardSlot Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the provisionedType of the card is not the same as presentType.
Name: CardRxAboveThreshold (620) Type: configurationAlarm (11) Probable cause: CardRxUtilizationCrossedAboveThreshold (460)	Severity: Major Object Type (class): CardSlot Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the card Rx exceeds the threshold value.
Name: CardRxTxAboveThreshold (621) Type: configurationAlarm (11) Probable cause: CardRxTxUtilizationCrossedAboveThreshold (461)	Severity: Major Object Type (class): CardSlot Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the card Tx exceeds the threshold value.
Name: cardTemperatureAboveOperatingThreshold (1178) Type: equipmentAlarm (3) Probable cause: fanNotWorking (879)	Severity: Major Object Type (class): CardSlot Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when card temperature raises above the threshold.
Name: cardTemperatureBelowOperatingThreshold (1179) Type: equipmentAlarm (3) Probable cause: airConditioningisHigh (880)	Severity: Major Object Type (class): CardSlot Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when card temperature falls below the threshold.

(4 of 17)

Alarm	Attributes	Description
Name: CardUnseated (1161) Type: equipmentAlarm (3) Probable cause: CardUnseated (864)	Severity: Major Object Type (class): CardSlot Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when card is removed.
Name: ClockFailure (1162) Type: communicationsAlarm (4) Probable cause: clockFailure (865)	Severity: Minor Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a clock failure occurs on MPT Radio.
Name: ConfigNotCompatible (405) Type: equipmentAlarm (3) Probable cause: DaughterCardConfigNotCompatible (301)	Severity: Critical Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when an MDA configuration is incompatible with the MDA.
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm (3) Probable cause: containingEquipmentAdministrativelyDown (330)	Severity: Minor Object Type (class): Port Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm (3) Probable cause: containingEquipmentMismatch (328)	Severity: Major Object Type (class): Port Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.
Name: ContainingEquipmentMissing (463) Type: equipmentAlarm (3) Probable cause: containingEquipmentMissing (327)	Severity: Major Object Type (class): Port Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMissing.
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm (3) Probable cause: containingEquipmentDown (329)	Severity: Major Object Type (class): Port Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.
Name: DataLossAlarm (148) Type: storageAlarm (25) Probable cause: dataLoss (122)	Severity: Major Object Type (class): FlashMemory Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device detects an error while writing to a compact flash unit.
Name: DaughterCardConfigNotCompatible (404) Type: equipmentAlarm (3) Probable cause: DaughterCardConfigNotCompatible (301)	Severity: Critical Object Type (class): DaughterCardSlot Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when a supported MDA is inserted into a compatible IOM slot, but the configuration on the MDA ports is not compatible with the MDA.
Name: DDMAux1HighAlarm (495) Type: thresholdAlarm (49) Probable cause: aux1HighAlarm (381)	Severity: Major Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP reaches the maximum threshold value.

(5 of 17)

Alarm	Attributes	Description
Name: DDMAux1HighWarning (494) Type: thresholdAlarm (49) Probable cause: aux1HighWarning (380)	Severity: Warning Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP approaches the maximum threshold value.
Name: DDMAux1LowAlarm (493) Type: thresholdAlarm (49) Probable cause: aux1LowAlarm (379)	Severity: Major Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP reaches the minimum threshold value.
Name: DDMAux1LowWarning (492) Type: thresholdAlarm (49) Probable cause: aux1LowWarning (378)	Severity: Warning Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP approaches the minimum threshold value.
Name: DDMAux2HighAlarm (499) Type: thresholdAlarm (49) Probable cause: aux2HighAlarm (385)	Severity: Major Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP reaches the maximum threshold value.
Name: DDMAux2HighWarning (498) Type: thresholdAlarm (49) Probable cause: aux2HighWarning (384)	Severity: Warning Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP approaches the maximum threshold value.
Name: DDMAux2LowAlarm (497) Type: thresholdAlarm (49) Probable cause: aux2LowAlarm (383)	Severity: Major Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP reaches the minimum threshold value.
Name: DDMAux2LowWarning (496) Type: communicatiothresholdAlarmnsAlarm (50) Probable cause: aux2LowWarning (382)	Severity: Warning Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP approaches the minimum threshold value.
Name: DDMRxOpticalPowerHighAlarm (491) Type: thresholdAlarm (49) Probable cause: rxOpticalPowerHighAlarm (377)	Severity: Major Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the received optical power of an SFP or XFP reaches the maximum threshold value.
Name: DDMRxOpticalPowerHighWarning (490) Type: thresholdAlarm (49) Probable cause: rxOpticalPowerHighWarning (376)	Severity: Warning Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the received optical power of an SFP or XFP approaches the maximum threshold value.

(6 of 17)

Alarm	Attributes	Description
Name: DDMRxOpticalPowerLowAlarm (489) Type: thresholdAlarm (49) Probable cause: rxOpticalPowerLowAlarm (375)	Severity: Major Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the received optical power of an SFP or XFP reaches the minimum threshold value.
Name: DDMRxOpticalPowerLowWarning (488) Type: thresholdAlarm (49) Probable cause: rxOpticalPowerLowWarning (374)	Severity: Warning Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the received optical power of an SFP or XFP approaches the minimum threshold value.
Name: DDMSupplyVoltageHighAlarm (479) Type: thresholdAlarm (49) Probable cause: supplyVoltageHighAlarm (365)	Severity: Major Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the supply voltage of an SFP or XFP reaches the maximum threshold value.
Name: DDMSupplyVoltageHighWarning (478) Type: thresholdAlarm (49) Probable cause: supplyVoltageHighWarning (364)	Severity: Warning Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the supply voltage of an SFP or XFP approaches the maximum threshold value.
Name: DDMSupplyVoltageLowAlarm (477) Type: thresholdAlarm (49) Probable cause: supplyVoltageLowAlarm (363)	Severity: Major Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the supply voltage of an SFP or XFP reaches the maximum threshold value.
Name: DDMSupplyVoltageLowWarning (476) Type: thresholdAlarm (49) Probable cause: supplyVoltageLowWarning (362)	Severity: Warning Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the supply voltage of an SFP or XFP approaches the maximum threshold value.
Name: DDMTemperatureHighAlarm (475) Type: thresholdAlarm (49) Probable cause: temperatureHighAlarm (361)	Severity: Major Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the temperature of an SFP or XFP reaches the maximum threshold value.
Name: DDMTemperatureHighWarning (474) Type: thresholdAlarm (49) Probable cause: temperatureHighWarning (360)	Severity: Warning Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the temperature of an SFP or XFP approaches the maximum threshold value.
Name: DDMTemperatureLowAlarm (473) Type: thresholdAlarm (49) Probable cause: temperatureLowAlarm (359)	Severity: Major Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the temperature of an SFP or XFP reaches the maximum threshold value.

(7 of 17)

Alarm	Attributes	Description
Name: DDMTemperatureLowWarning (472) Type: thresholdAlarm (49) Probable cause: temperatureLowWarning (358)	Severity: Warning Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the temperature of an SFP or XFP approaches the maximum threshold value.
Name: DDMTxBiasCurrentHighAlarm (483) Type: thresholdAlarm (49) Probable cause: txBiasCurrentHighAlarm (369)	Severity: Major Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the transmit bias current of an SFP or XFP reaches the maximum threshold value.
Name: DDMTxBiasCurrentHighWarning (482) Type: thresholdAlarm (49) Probable cause: txBiasCurrentHighWarning (368)	Severity: Warning Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the transmit bias current of an SFP or XFP approaches the maximum threshold value.
Name: DDMTxBiasCurrentLowAlarm (481) Type: thresholdAlarm (49) Probable cause: txBiasCurrentLowAlarm (367)	Severity: Major Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the transmit bias current of an SFP or XFP reaches the maximum threshold value.
Name: DDMTxBiasCurrentLowWarning (480) Type: thresholdAlarm (49) Probable cause: txBiasCurrentLowWarning (366)	Severity: Warning Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the transmit bias current of an SFP or XFP approaches the maximum threshold value.
Name: DDMTxOutputPowerHighAlarm (487) Type: thresholdAlarm (49) Probable cause: txOutputPowerHighAlarm (373)	Severity: Major Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the output power of an SFP or XFP reaches the maximum threshold value.
Name: DDMTxOutputPowerHighWarning (486) Type: thresholdAlarm (49) Probable cause: txOutputPowerHighWarning (372)	Severity: Warning Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the output power of an SFP or XFP approaches the maximum threshold value.
Name: DDMTxOutputPowerLowAlarm (485) Type: thresholdAlarm (49) Probable cause: txOutputPowerLowAlarm (371)	Severity: Major Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the output power of an SFP or XFP reaches the maximum threshold value.
Name: DDMTxOutputPowerLowWarning (484) Type: thresholdAlarm (49) Probable cause: txOutputPowerLowWarning (370)	Severity: Warning Object Type (class): DigitalDiagnosticMonitoring Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the output power of an SFP or XFP approaches the maximum threshold value.

(8 of 17)

Alarm	Attributes	Description
Name: Degrade (622) Type: communicationsAlarm (4) Probable cause: degrade (462)	Severity: Major Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a degraded signal is detected.
Name: DialogFailure (1163) Type: communicationsAlarm (4) Probable cause: dialogFailure (866)	Severity: Minor Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a MPT temporary communication failure occurs.
Name: DiskCapacityProblem (144) Type: storageAlarm (25) Probable cause: diskCapacityProblem (115)	Severity: Variable or indeterminate Object Type (class): FlashMemory Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when a compact flash capacity threshold value on an NE is reached or exceeded. The alarm condition is detected during resynchronization or when a tnmxEqFlashDiskFull trap is received. The threshold value is not configurable.The severity of the alarm depends on the percentage of disk capacity used, as listed below:- 75 percent, Minor- 90 percent, Major- 100 percent, Critical
Name: downgradedCardAlarm (256) Type: softwareAlarm (19) Probable cause: downgradedCard (195)	Severity: Warning Object Type (class): Card Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.
Name: DryContactAlarm (460) Type: dryContactAlarm (47) Probable cause: dryContactExternalAlarmRaised (351)	Severity: Variable or indeterminate Object Type (class): DryContact Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when a device detects a dry contact alarm condition.
Name: DuplicateRole (470) Type: configurationAlarm (11) Probable cause: twoElementsWithSameRole (356)	Severity: Major Object Type (class): StackConfiguration Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when a slot has the same primary or secondary role as another slot in the stack. The slot subsequently enters pass-through mode.
Name: DuplicateSlot (468) Type: configurationAlarm (11) Probable cause: duplicateSlotNINumber (354)	Severity: Major Object Type (class): StackConfiguration Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when a slot has the same slot number as another stack element. The slot must relinquish its operational status because it has a higher election key, based on the up time, slot number, and MAC address. Both slots subsequently enter pass-through mode.
Name: DyingGasp (1164) Type: communicationsAlarm (4) Probable cause: dyingGaspSignal (463)	Severity: Major Object Type (class): CardSlot Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when a Dying Gasp trap is received to indicate a power failure.
Name: DyingGaspSignal (623) Type: communicationsAlarm (4) Probable cause: dyingGaspSignal (463)	Severity: Major Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when a Dying Gasp signal is received from a remote 7210 SAS to indicate a power loss.

(9 of 17)

Alarm	Attributes	Description
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm (3) Probable cause: equipmentAdministrativelyDown (326)	Severity: Minor Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.
Name: EquipmentDegraded (604) Type: equipmentAlarm (3) Probable cause: singleFanFailure (450)	Severity: Minor Object Type (class): FanTray Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.
Name: EquipmentDown (10) Type: equipmentAlarm (3) Probable cause: inoperableEquipment (8)	Severity: Major Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.
Name: EquipmentFailure (145) Type: equipmentAlarm (3) Probable cause: cardFailure (123)	Severity: Critical Object Type (class): ReplaceableUnit Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.
Name: EquipmentInTest (11) Type: equipmentAlarm (3) Probable cause: equipmentInTest (9)	Severity: Warning Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when equipment enters a diagnostic state.
Name: EquipmentMismatch (9) Type: equipmentAlarm (3) Probable cause: equipmentTypeMismatch (7)	Severity: Major Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.
Name: EquipmentRemoved (8) Type: equipmentAlarm (3) Probable cause: replaceableEquipmentRemoved (6)	Severity: Major Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.
Name: ExcessiveEnvironmentTemparature (1118) Type: communicationsAlarm (4) Probable cause: excessiveEnvironmentTemp (830)	Severity: Major Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when MPT is overheated.
Name: FanFailure (624) Type: equipmentAlarm (3) Probable cause: fanFailure (116)	Severity: Critical Object Type (class): FanTray Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the associated fan is not operationally Up.

(10 of 17)

Alarm	Attributes	Description
Name: FanRPMAlarm (1126) Type: equipmentAlarm (3) Probable cause: fanFailure (116)	Severity: Info Object Type (class): Fan Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the associated fan alarm usage state is not set to Normal.
Name: FanTrayRemoved (569) Type: equipmentAlarm (3) Probable cause: FanTrayRemoved (438)	Severity: Critical Object Type (class): FanTray Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.
Name: FIBHighOccupancy (752) Type: resourceAlarm (28) Probable cause: FIBHighOccupancy (528)	Severity: Warning Object Type (class): BaseCard Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the FIB occupancy on an IOM card changes from normal to high.
Name: FibOutOfSynch (625) Type: resourceAlarm (28) Probable cause: fibUpdateFailed (464)	Severity: Critical Object Type (class): DaughterCard Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the FIB on an MDA is out of synchronization.
Name: FirmwareDownloadOnGoing (626) Type: equipmentAlarm (3) Probable cause: firmwareDownloadOnGoing (465)	Severity: Warning Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a firmware download is in progress.
Name: FirmwareMismatchAlarm (146) Type: firmwareAlarm (26) Probable causes: • bootRomVersionMismatch (119) • fpgaVersionMismatch (120)	Severity: Critical Object Type (class): Card Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device detects a mismatch between the firmware version and the device software image. The alarm information includes the expected firmware version.
Name: FirmwareUpgradeAlarm (212) Type: firmwareAlarm (26) Probable cause: firmwareUpgraded (169)	Severity: Info Object Type (class): Card Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when a device automatically upgrades the firmware of a hot-inserted IOM or CPM.
Name: HardwareRedundancyAlarm (147) Type: equipmentAlarm (3) Probable cause: primaryCpmFailure (121)	Severity: Major Object Type (class): ControlProcessor Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the primary CPM fails.
Name: HouseKeeping (1165) Type: equipmentAlarm (3) Probable cause: houseKeeping (867)	Severity: Major Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a HouseKeeping trap is received.
Name: IncompatibleCapacity (1166) Type: communicationsAlarm (4) Probable cause: incompatibleCapacity (868)	Severity: Major Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when there is an incompatibility in radio capacity.
Name: IncompatibleChannelSpacing (1167) Type: communicationsAlarm (4) Probable cause: incompatibleChannelSpacing (869)	Severity: Minor Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when there is a compatibility problem in channel spacing.

(11 of 17)

Alarm	Attributes	Description
Name: InternalCommunicationProblem (627) Type: equipmentAlarm (3) Probable cause: internalCommunicationProblem (466)	Severity: Major Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an ODU is unresponsive.
Name: LagPortAddFailed (422) Type: equipmentAlarm (3) Probable cause: linkDown (315)	Severity: Warning Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the Lag Port Add function Fails.
Name: LanFailure (628) Type: equipmentAlarm (3) Probable cause: lanFailure (467)	Severity: Major Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a LAN failure is detected.
Name: LinkDown (12) Type: communicationsAlarm (4) Probable cause: portLinkProblem (10)	Severity: Major Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a port has no associated physical link.
Name: LossOfAlignment (629) Type: communicationsAlarm (4) Probable cause: lossOfAlignment (468)	Severity: Minor Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a Loss of Alignment signal is detected.
Name: LossOfCESoEthFrames (1168) Type: communicationsAlarm (4) Probable cause: lossOfCESoEthFrames (870)	Severity: Minor Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a loss occurs on CES over Ethernet Frames.
Name: LossOfFrame (630) Type: communicationsAlarm (4) Probable cause: lossOfFrame (97)	Severity: Major Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a port receives a Loss Of Frame signal.
Name: LossOfProtection (1169) Type: communicationsAlarm (4) Probable cause: lossOfProtection (871)	Severity: Minor Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a protection loss occurs on MPT Radio.
Name: LossOfSignal (631) Type: communicationsAlarm (4) Probable cause: lossOfSignal (99)	Severity: Major Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a Loss of Signal signal is detected on a PDH tributary.
Name: LowTemperatureDetected (1127) Type: environmentalAlarm (2) Probable cause: equipmentOvercooled (838)	Severity: Major Object Type (class): Shelf Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the chassis temperature exceeds the maximum threshold value.
Name: LowTemperatureThresholdCrossed (1128) Type: environmentalAlarm (2) Probable cause: equipmentOvercooled (838)	Severity: Major Object Type (class): Environment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a temperature crosses a threshold.

(12 of 17)

Alarm	Attributes	Description
Name: MigrationCompleted (753) Type: migrationComplete (62) Probable cause: migrationComplete (529)	Severity: Info Object Type (class): NeCardSwapTask Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when a card migration event completes.
Name: MigrationFailed (754) Type: migrationFailure (63) Probable cause: migrationFailure (530)	Severity: Major Object Type (class): NeCardSwapTask Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when a card migration event fails.
Name: ModFail (1171) Type: communicationsAlarm (4) Probable cause: modFail (872)	Severity: Major Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a modulation failure occurs.
Name: ModLOS (1172) Type: communicationsAlarm (4) Probable cause: modLOS (873)	Severity: Major Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a loss of signal in modulation occurs.
Name: MPTPowerSupplyFailure (1170) Type: equipmentAlarm (3) Probable cause: powerSupplyFailure (117)	Severity: Major Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a power supply failure occurs on MPT Radio Power Source.
Name: OutOfSlots (462) Type: configurationAlarm (11) Probable cause: noAvailableSlotNumbers (352)	Severity: Major Object Type (class): Shelf Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when a stack element enters pass-through mode because there is no slot number for the element.
Name: OverTemperatureDetected (388) Type: environmentalAlarm (2) Probable cause: equipmentOverheated (5)	Severity: Major Object Type (class): Shelf Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the chassis temperature exceeds the maximum threshold value.
Name: PChipCAMEvent (814) Type: hardwareAnomaly (55) Probable cause: camError (577)	Severity: Warning Object Type (class): Card Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an IOM or CPM experiences a P-chip CAM error.
Name: PChipError (593) Type: hardwareAnomaly (55) Probable cause: pChipError (447)	Severity: Warning Object Type (class): BaseCard Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a P chip reports persistent errors on the specified complex in the specified direction.
Name: PChipMemoryEvent (608) Type: hardwareAnomaly (55) Probable cause: memoryParityError (451)	Severity: Warning Object Type (class): BaseCard Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a P chip detects a memory parity error. The alarm is raised against a 7450 ESS, 7710 SR, or 7750 SR. The alarm is raised against a Release 6.0 NE at R10 or later and a Release 6.1 NE at R5 or later.

(13 of 17)

Alarm	Attributes	Description
Name: PowerSupplyFailure (633) Type: equipmentAlarm (3) Probable cause: powerSupplyFailure (117)	Severity: Critical Object Type (class): PowerSupplyTray Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.
Name: PowerSupplyRemoved (542) Type: equipmentAlarm (3) Probable cause: PowerSupplyRemoved (415)	Severity: Critical Object Type (class): PowerSupplyTray Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a chassis power supply is removed.
Name: PowerSupplyVoltageAlarm (1129) Type: equipmentAlarm (3) Probable cause: powerSupplyFailure (117)	Severity: Info Object Type (class): PowerSupply Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the associated power supply alarm voltage state is not set to Normal.
Name: PPPFail (632) Type: communicationsAlarm (4) Probable cause: pppFail (469)	Severity: Warning Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a PPP IP Fail condition is detected.
Name: PrimaryPathLimitReached (457) Type: resourceAlarm (28) Probable cause: resourceLimitReached (131)	Severity: Warning Object Type (class): DaughterCard Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the primary path bandwidth limit is reached.
Name: ProvisioningMismatch (634) Type: equipmentAlarm (3) Probable cause: provisioningMismatch (470)	Severity: Major Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a license mismatch is detected for provisioned equipment.
Name: RemoteNEFailure (1173) Type: equipmentAlarm (3) Probable cause: remoteNEFailure (874)	Severity: Warning Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when there is a failure in the remote network element.
Name: ReplaceableUnitMissing (635) Type: equipmentAlarm (3) Probable cause: cardMissing (471)	Severity: Major Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device detects that a provisioned card is not physically present.
Name: ReplaceableUnitProblem (636) Type: equipmentAlarm (3) Probable cause: cardFail (472)	Severity: Major Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a card fails.
Name: ReplaceableUnitTypeMismatch (637) Type: equipmentAlarm (3) Probable cause: equipmentMismatch (473)	Severity: Major Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when there is a mismatch between the installed card type and the expected card type.

(14 of 17)

Alarm	Attributes	Description
Name: RetimingBufferOverFlow (1130) Type: communicationsAlarm (4) Probable cause: bufferOverFlow (839)	Severity: Minor Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an retiming buffer overflow occurs.
Name: SecondaryPathLimitReached (458) Type: resourceAlarm (28) Probable cause: resourceLimitReached (131)	Severity: Warning Object Type (class): DaughterCard Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the secondary path bandwidth limit is reached.
Name: SGLimitExceeded (456) Type: resourceAlarm (28) Probable cause: pimSnpgSGGroupMaxSupportedLimitExceeded (350)	Severity: Warning Object Type (class): Card Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the number of PIM snooping source group records on a card exceeds the maximum.
Name: ShelfCPUAboveThreshold (638) Type: configurationAlarm (11) Probable cause: ShelfCPUUtilizationCrossedAboveThreshold (474)	Severity: Major Object Type (class): HealthMonitoring Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when shelf CPU usage exceeds the threshold value.
Name: ShelfMemoryAboveThreshold (639) Type: configurationAlarm (11) Probable cause: ShelfMemoryUtilizationCrossedAboveThreshold (475)	Severity: Major Object Type (class): HealthMonitoring Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when shelf memory usage exceeds the threshold value.
Name: ShelfRxAboveThreshold (640) Type: configurationAlarm (11) Probable cause: ShelfRxUtilizationCrossedAboveThreshold (476)	Severity: Major Object Type (class): HealthMonitoring Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when shelf Rx exceeds the threshold value.
Name: ShelfRxTxAboveThreshold (641) Type: configurationAlarm (11) Probable cause: ShelfRxTxUtilizationCrossedAboveThreshold (477)	Severity: Major Object Type (class): HealthMonitoring Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when shelf Tx exceeds the threshold value.
Name: ShelfTemperatureAboveThreshold (642) Type: configurationAlarm (11) Probable cause: ShelfTemperatureUtilizationCrossedAboveThreshold (478)	Severity: Major Object Type (class): HealthMonitoring Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when shelf temperature exceeds the threshold value.
Name: SoftwareFailureAlarm (149) Type: softwareAlarm (19) Probable cause: loadFailed (124)	Severity: Critical Object Type (class): ReplaceableUnit Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the CPM fails to load the software from the specified location. The alarm information includes the software location.
Name: SSHServerPreserveKeyFailure (406) Type: softwareAlarm (19) Probable cause: preserveKeyFailure (302)	Severity: Critical Object Type (class): FlashMemory Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when the CPM fails to save the SSH server host key on the persistent drive.

(15 of 17)

Alarm	Attributes	Description
Name: StandbyVersionMismatch (1174) Type: equipmentAlarm (3) Probable cause: standbyVersionMismatch (875)	Severity: Minor Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when there is a mismatch in the Standby Version of the node software.
Name: SWIncompatibility (471) Type: configurationAlarm (11) Probable cause: elementNotCompatibleWithExistingStack (357)	Severity: Major Object Type (class): StackConfiguration Domain: equipment Implicitly cleared (self-clearing): No	The alarm is raised when a slot is not compatible with the current stack. The slot subsequently enters pass-through mode.
Name: SychronizationLossOfSignal (799) Type: communicationsAlarm (4) Probable cause: lossOfSignal (99)	Severity: Major Object Type (class): Shelf Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an SLOS signal is detected on a PDH tributary.
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm (2) Probable cause: equipmentOverheated (5)	Severity: Major Object Type (class): Environment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a temperature crosses a threshold.
Name: TemporaryCommunicationFailure (800) Type: equipmentAlarm (3) Probable cause: temporaryCommunicationProblem (566)	Severity: Major Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a temporary communication failure is detected.
Name: ThresholdCrossingAlarm (14) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Minor Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a port value crosses a threshold.
Name: TxFail (1175) Type: communicationsAlarm (4) Probable cause: txFail (876)	Severity: Major Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a transmitter failure occurs.
Name: UnavailableTime (644) Type: communicationsAlarm (4) Probable cause: unavailableTime (480)	Severity: Major Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a port experiences 10 consecutive SES.
Name: UnconfiguredEquipmentPresent (645) Type: equipmentAlarm (3) Probable cause: unconfiguredEquipmentPresent (481)	Severity: Warning Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when unconfigured equipment is detected.
Name: UnderlyingResourceDegrade (1176) Type: communicationsAlarm (4) Probable cause: underlyingResourceDegrade (877)	Severity: Minor Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an underlying resource degrade happens on the radio interface.

(16 of 17)

Alarm	Attributes	Description
Name: UnderlyingResourceUnavailable (1131) Type: communicationsAlarm (4) Probable cause: underlyingResourceUnavailable (724)	Severity: Minor Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an underlying resource is unavailable on an E1, radio, or Ethernet interface.
Name: UnderlyingResourceUnavailableService (1177) Type: communicationsAlarm (4) Probable cause: underlyingResourceUnavailableService (878)	Severity: Minor Object Type (class): PhysicalPort Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an underlying resource service is unavailable on an E1, radio, or Ethernet interface.
Name: upgradedCardAlarm (255) Type: softwareAlarm (19) Probable cause: upgradedCard (194)	Severity: Warning Object Type (class): Card Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.
Name: VersionMismatch (646) Type: equipmentAlarm (3) Probable cause: versionMismatch (405)	Severity: Minor Object Type (class): Equipment Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an ODU software version mismatch is detected.
Name: XplError (573) Type: hardwareAnomaly (55) Probable cause: xplError (443)	Severity: Warning Object Type (class): DaughterCard Domain: equipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an MDA reports persistent XPL Errors.

(17 of 17)

Table 3-17 Domain: ethernetequipment

Alarm	Attributes	Description
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm (11) Probable cause: ethernetPortConfiguredLoopback (567)	Severity: Warning Object Type (class): EthernetPortSpecifics Domain: ethernetequipment Implicitly cleared (self-clearing): No	The alarm is raised when a timed loopback is in effect for an Ethernet port.
Name: EthernetPortHighBer (307) Type: communicationsAlarm (4) Probable cause: HighBer (238)	Severity: Major Object Type (class): EthernetPortSpecifics Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a high bit-error rate on an Ethernet port.
Name: EthernetPortLocalFault (305) Type: communicationsAlarm (4) Probable cause: LocalFault (236)	Severity: Major Object Type (class): EthernetPortSpecifics Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a local fault on an Ethernet port.

(1 of 6)

Alarm	Attributes	Description
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm (4) Probable cause: NoFrameLock (237)	Severity: Major Object Type (class): EthernetPortSpecifics Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports No Frame Lock on an Ethernet port.
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm (4) Probable cause: RemoteFault (235)	Severity: Major Object Type (class): EthernetPortSpecifics Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a remote fault on an Ethernet port.
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm (4) Probable cause: SignalFailure (234)	Severity: Major Object Type (class): EthernetPortSpecifics Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a signal failure on an Ethernet port.
Name: OpticalAmplifierLossOfInputOpticalPower (1185) Type: communicationsAlarm (4) Probable cause: AmplifierLossOfInputOpticalPower (886)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a Amplifier Loss of input optical power optical amplifier interface.
Name: OpticalAmplifierLossOfOutputPower (1186) Type: communicationsAlarm (4) Probable cause: AmplifierLossOfOutputPower (887)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a Amplifier Loss of output power on a optical amplifier interface.
Name: OPticalAmplifierModuleCaseTemperatureHigh (1180) Type: communicationsAlarm (4) Probable cause: AmplifierModuleCaseTemperatureHigh (881)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an Amplifier Module Case Temperature High on a optical amplifier interface.
Name: OPticalAmplifierModuleCaseTemperatureLow (1181) Type: communicationsAlarm (4) Probable cause: AmplifierModuleCaseTemperatureLow (882)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a Amplifier Module Case Temperature Low on a optical amplifier interface.
Name: OpticalAmplifierModuleCommunicationFailure (1187) Type: communicationsAlarm (4) Probable cause: AmplifierModuleCommunicationFailure (888)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a Amplifier Module communication failure on a tunable dispersion compensation module's interface.
Name: OpticalAmplifierPumpCurrent (1188) Type: communicationsAlarm (4) Probable cause: AmplifierPumpcurrent (889)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an Amplifier Pump over current on a optical amplifier interface.

(2 of 6)

Alarm	Attributes	Description
Name: OPticalAmplifierPumpTemperature (1182) Type: communicationsAlarm (4) Probable cause: AmplifierPumpTemperature (883)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an Amplifier Pump Temperature on a optical amplifier interface.
Name: OpticalTdcmEEPROMinvalid (1189) Type: communicationsAlarm (4) Probable cause: TdcmEEPROMinvalid (890)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a Tdcm EEPROM invalid on a tunable dispersion compensation module's interface.
Name: OpticalTdcmModuleCommunicationFailure (1190) Type: communicationsAlarm (4) Probable cause: TdcmModuleCommunicationFailure (891)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a Tdcm Module Communication Failure on a tunable dispersion compensation module's interface.
Name: OPticalTdcmModuleTemperatureHigh (1183) Type: communicationsAlarm (4) Probable cause: TdcmModuleTemperatureHigh (884)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an Tdcm Module Temperature High on a tunable dispersion compensation module's interface.
Name: OPticalTdcmModuleTemperatureLow (1184) Type: communicationsAlarm (4) Probable cause: TdcmModuleTemperatureLow (885)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an Tdcm Module Temperature Low on a tunable dispersion compensation module's interface.
Name: OpticalTdcmNotReady (1191) Type: communicationsAlarm (4) Probable cause: TdcmNotReady (892)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an Tdcm not Ready on a tunable dispersion compensation module's interface.
Name: OpticalTdcmThermalControlTemperatureLimit (1192) Type: communicationsAlarm (4) Probable cause: TdcmThermalControlTemperatureLimit (893)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a Tdcm thermal control temperature limit on a tunable dispersion compensation module's interface.
Name: OpticalTdcmThermalControlUnlocked (1193) Type: communicationsAlarm (4) Probable cause: TdcmThermalControlUnlocked (894)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a Tdcm Thermal Control Unlocked on a tunable dispersion compensation module's interface.
Name: OTUAlarmIndicationSignal (755) Type: communicationsAlarm (4) Probable cause: AlarmIndicationSignal (531)	Severity: Major Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an AIS on an OTU-enabled interface.

(3 of 6)

Alarm	Attributes	Description
Name: OTUBackwardDefectIndication (756) Type: communicationsAlarm (4) Probable cause: BackwardDefectIndication (532)	Severity: Major Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a BDI on an OTU-enabled interface.
Name: OTUBackwardIncomingAlignmentError (815) Type: communicationsAlarm (4) Probable cause: BackwardIncomingAlignmentError (578)	Severity: Major Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an ODU alarm indication signal on an OTU-enabled interface.
Name: OTUBitErrorRateSignalDegradation (757) Type: communicationsAlarm (4) Probable cause: BitErrorRateSignalDegradation (533)	Severity: Major Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a BER-SD on an OTU-enabled interface.
Name: OTUBitErrorRateSignalFail (758) Type: communicationsAlarm (4) Probable cause: BitErrorRateSignalFail (534)	Severity: Critical Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a BER-SF on an OTU-enabled interface.
Name: OTUFECRxTxModeMismatch (759) Type: communicationsAlarm (4) Probable cause: FECRxTxModeMismatch (535)	Severity: Critical Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a FEC Rx/Tx mode mismatch on an OTU-enabled interface.
Name: OTUFECSignalDegradation (760) Type: communicationsAlarm (4) Probable cause: FECSignalDegradation (536)	Severity: Major Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a FEC-SD on an OTU-enabled interface.
Name: OTUFECSignalFailure (761) Type: communicationsAlarm (4) Probable cause: FECSignalFailure (537)	Severity: Major Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a FEC-SF on an OTU-enabled interface.
Name: OTUIncomingAlignmentError (816) Type: communicationsAlarm (4) Probable cause: IncomingAlignmentError (579)	Severity: Major Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an ODU open connection indication on an OTU-enabled interface.
Name: OTULossOfClock (762) Type: communicationsAlarm (4) Probable cause: LossOfClock (538)	Severity: Critical Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an LOC on an OTU-enabled interface.
Name: OTULossOfFraming (763) Type: communicationsAlarm (4) Probable cause: LossOfFraming (539)	Severity: Critical Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an LOF on an OTU-enabled interface.
Name: OTULossOfMultiFrame (764) Type: communicationsAlarm (4) Probable cause: LossOfMultiFrame (540)	Severity: Major Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an LOM on an OTU-enabled interface.

(4 of 6)

Alarm	Attributes	Description
Name: OTULossOfSignal (765) Type: communicationsAlarm (4) Probable cause: LossOfSignal (541)	Severity: Critical Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an LOS on an OTU-enabled interface.
Name: OTUODUAlarmIndicationSignal (766) Type: communicationsAlarm (4) Probable cause: ODUAlarmIndicationSignal (542)	Severity: Major Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an ODU AIS on an OTU-enabled interface.
Name: OTUODULocked (767) Type: communicationsAlarm (4) Probable cause: ODULocked (543)	Severity: Critical Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an ODU locked on an OTU-enabled interface.
Name: OTUODUOpenConnectionIndication (768) Type: communicationsAlarm (4) Probable cause: ODUOpenConnectionIndication (544)	Severity: Critical Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an ODU-OCI on an OTU-enabled interface.
Name: OTUOPUPSIPayloadTypeMismatch (817) Type: communicationsAlarm (4) Probable cause: OPUPSIPayloadTypeMismatch (580)	Severity: Major Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a PM backward defect indication on an OTU-enabled interface.
Name: OTUOPUPSITraceMismatch (818) Type: communicationsAlarm (4) Probable cause: OPUPSITraceMismatch (581)	Severity: Major Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an ODU locked indication on an OTU-enabled interface.
Name: OTUPMBackwardDefectIndication (769) Type: communicationsAlarm (4) Probable cause: PMBackwardDefectIndication (545)	Severity: Major Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a PM BDI on an OTU-enabled interface.
Name: OTUPMTraceIDMismatch (819) Type: communicationsAlarm (4) Probable cause: PMTraceIDMismatch (582)	Severity: Major Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an ODU open connection indication on an OTU-enabled interface.
Name: OTUTraceIdMismatch (820) Type: communicationsAlarm (4) Probable cause: TraceIdMismatch (583)	Severity: Major Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a trace ID mismatch on an OTU-enabled interface.
Name: OTUUncorrectableFECErrors (770) Type: communicationsAlarm (4) Probable cause: UncorrectableFECErrors (546)	Severity: Major Object Type (class): OtuInterface Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports one or more uncorrectable FEC errors on an OTU-enabled interface.

(5 of 6)

Alarm	Attributes	Description
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected (48) Probable cause: HighBer (238)	Severity: Major Object Type (class): EthernetPortSpecifics Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device detects a physical loop on an Ethernet port.
Name: WaveTrackerEncoderDegrade (821) Type: communicationsAlarm (4) Probable cause: EncoderDegrade (584)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an encoder degradation on a wavelength tracker interface.
Name: WaveTrackerEncoderFailure (822) Type: communicationsAlarm (4) Probable cause: EncoderFailure (585)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports an encoder failure on a wavelength tracker interface.
Name: WaveTrackerPowerControlDegrade (823) Type: communicationsAlarm (4) Probable cause: PowerControlDegrade (586)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a power control degradation on a wavelength tracker interface.
Name: WaveTrackerPowerControlFailure (824) Type: communicationsAlarm (4) Probable cause: PowerControlFailure (587)	Severity: Critical Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a power control failure on a wavelength tracker interface.
Name: WaveTrackerPowerControlHighlimit (825) Type: communicationsAlarm (4) Probable cause: PowerControlHighlimit (588)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a power control high limit on a wavelength tracker interface.
Name: WaveTrackerPowerControllowlimit (826) Type: communicationsAlarm (4) Probable cause: PowerControllowlimit (589)	Severity: Major Object Type (class): WaveLengthTracker Domain: ethernetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a power control low limit on a wavelength tracker interface.

(6 of 6)

Table 3-18 Domain: ethernetoam

Alarm	Attributes	Description
Name: DualEndedLossNotSupported (1194) Type: oamAlarm (18) Probable cause: dualEndedLossNotSupported (895)	Severity: Warning Object Type (class): MaintAssociation Domain: ethernetoam Implicitly cleared (self-clearing): Yes	The alarm is raised when at least one MEP that does not support Y1731 Dual Ended Loss test isparticipating in aCFM Continuity Check test that has Y1731 Dual Ended Loss test enabled.

(1 of 2)

Alarm	Attributes	Description
Name: DualEndedLossThresholdAlarm (1195) Type: oamAlarm (18) Probable cause: dualEndedLossThresholdExceeded (896)	Severity: Minor Object Type (class): Mep Domain: ethernetoam Implicitly cleared (self-clearing): Yes	The alarm is raised when a MEP reports that either the Local or Remote loss ratio has exceededthe configured thresholdfor the specified remote MEP.
Name: RemoteMepCCMAlarm (502) Type: oamAlarm (18) Probable cause: missingRemoteMep (388)	Severity: Major Object Type (class): Mep Domain: ethernetoam Implicitly cleared (self-clearing): Yes	The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEPDB State tab on a MEP lists the missing remote MEPs.
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm (18) Probable cause: networkDegradation (204)	Severity: Major Object Type (class): MaintAssociation Domain: ethernetoam Implicitly cleared (self-clearing): Yes	The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.

(2 of 2)

Table 3-19 Domain: ethernettunnel

Alarm	Attributes	Description
Name: apsCfgRaiseAlarm (772) Type: configurationAlarm (11) Probable cause: configurationMismatch (548)	Severity: Major Object Type (class): EthernetTunnelEndpoint Domain: ethernettunnel Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects a mismatch between the working and protection Ethernet tunnel group configurations.
Name: apsNoRspRaiseAlarm (773) Type: configurationAlarm (11) Probable cause: incompleteProtectionSwitching (549)	Severity: Major Object Type (class): EthernetTunnelEndpoint Domain: ethernettunnel Implicitly cleared (self-clearing): Yes	The alarm is raised when an Ethernet tunnel group protection switch is incomplete, as indicated by a comparison of the transmitted 'Requested Signal' values and the received 'Bridged Signal' in the APS protocol.
Name: apsPrvsnRaiseAlarm (774) Type: configurationAlarm (11) Probable cause: provisioningMismatch (470)	Severity: Major Object Type (class): EthernetTunnelEndpoint Domain: ethernettunnel Implicitly cleared (self-clearing): Yes	The alarm is raised when an Ethernet tunnel group provisioning mismatch is detected at the ETH layer. The mismatch is detected through a comparison of the transmitted and received APS protocol A, B and D bits.
Name: EthernetTunnelDown (771) Type: configurationAlarm (11) Probable cause: ethernetTunnelDown (547)	Severity: Major Object Type (class): EthernetTunnel Domain: ethernettunnel Implicitly cleared (self-clearing): Yes	The alarm is raised when the aggregated Ethernet tunnel Operational State is Down.

Table 3-20 Domain: ethring

Alarm	Attributes	Description
Name: apsPrvsnAlarm (1196) Type: configurationAlarm (11) Probable cause: provisioningMismatch (470)	Severity: Major Object Type (class): Element Domain: ethring Implicitly cleared (self-clearing): Yes	The alarm is raised when an an Ethernet RIng provisioning mismatch is detected.A mismatch occurs when the RPL Owner Node receives one or more No Request R-APSmessage(s) with RPL Blocked status flag set (NR, RB) and a Node ID that differs for its own.

Table 3-21 Domain: file

Alarm	Attributes	Description
Name: LogLocFailure (340) Type: storageAlarm (25) Probable causes: • AdminLocFailure (244) • BackupLocFailure (245)	Severity: Variable or indeterminate Object Type (class): Policy Domain: file Implicitly cleared (self-clearing): No	The alarm is raised when an attempt to create a log or billing file fails. The probable cause is AdminLocFailure when using the admin location fails, in which case the backup location, if specified, is used. The probable cause is BackupLocFailure when using the backup location fails.

Table 3-22 Domain: generic

Alarm	Attributes	Description
Name: DeploymentFailure (13) Type: deploymentFailure (5) Probable cause: failedToModifyNetworkResource (11)	Severity: Minor Object Type (class): GenericObject Domain: generic Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM is unable to create, modify, or delete a network object because of NE unreachability or a failed SNMP set operation. The alarm information includes the deployment ID, the requesting user ID, and the deployment type.
Name: ThresholdCrossingAlarm (14) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): GenericObject Domain: generic Implicitly cleared (self-clearing): Yes	The alarm is raised when a monitored object statistics-counter value exceeds a threshold value in the associated statistics policy.
Name: ThresholdCrossingAlarmDbl (226) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): GenericObject Domain: generic Implicitly cleared (self-clearing): Yes	The alarm is raised when a value crosses a configured rising or falling threshold. The alarm information includes the current threshold value, the default threshold value, and the threshold name.

Table 3-23 Domain: genericne

Alarm	Attributes	Description
Name: GenericInterfaceLinkDown (403) Type: equipmentAlarm (3) Probable cause: inoperableEquipment (8)	Severity: Major Object Type (class): GenericNeInterface Domain: genericne Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects a communication link failure on a GNE interface. The alarm clears when the link returns to service.

Table 3-24 Domain: igh

Alarm	Attributes	Description
Name: IGHMisconfigured (827) Type: ighAlarm (74) Probable cause: IGHProtocolMismatch (590)	Severity: Major Object Type (class): InterfaceGroupHandler Domain: igh Implicitly cleared (self-clearing): Yes	The alarm is raised when the IGH is administratively up but none of the IGH protocols is operationally up.

Table 3-25 Domain: igmp

Alarm	Attributes	Description
Name: CModeRxQueryMismatch (160) Type: configurationAlarm (11) Probable cause: InvalidCompatibilityModeofQueryReceieved (130)	Severity: Major Object Type (class): Interface Domain: igmp Implicitly cleared (self-clearing): No	The alarm is raised when an IGMP interface receives an IGMP query of a higher version than the version configured on the interface, for example, when the interface is configured for IGMPv1 and it receives an IGMPv2 or IGMPv3 query. The interface does not process the received IGMP message.
Name: IgmpDown (158) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): Site Domain: igmp Implicitly cleared (self-clearing): Yes	The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.
Name: McacPolicyDropped (341) Type: communicationsAlarm (4) Probable cause: igmpGroupOnSapDropped (246)	Severity: Major Object Type (class): Interface Domain: igmp Implicitly cleared (self-clearing): No	The alarm is raised when an IGMP group is dropped because a multicast CAC policy is applied.
Name: QueryVerMismatch (159) Type: configurationAlarm (11) Probable cause: InvalidVersionofQueryMessageReceived (129)	Severity: Warning Object Type (class): Interface Domain: igmp Implicitly cleared (self-clearing): No	The alarm is raised when an interface configured for IGMPv3 receives a query message for an earlier IGMP version. The interface subsequently enters an IGMP mode that is compatible with the earlier version. The alarm information includes the IGMP version on the interface and the IGMP version of the received query.

Table 3-26 Domain: ipipe

Alarm	Attributes	Description
Name: CeAddressIncompatible (251) Type: configurationAlarm (11) Probable cause: ceAddressIncompatible (190)	Severity: Major Object Type (class): Ipipe Domain: ipipe Implicitly cleared (self-clearing): Yes	The alarm is raised when two SAPs in an Ipipe have the same CE IP address, or when the CE IP address is not the same as the CE IP address of the peer SDP binding.

Table 3-27 Domain: ipsec

Alarm	Attributes	Description
Name: CorporateAndSecuredCompositeServicesAreNotConnected (828) Type: serviceAlarm (16) Probable cause: CompositeServiceMisconfiguration (591)	Severity: Warning Object Type (class): IPSecSecuredVpn Domain: ipsec Implicitly cleared (self-clearing): No	The alarm is raised when the corporate and secured services used by an IPsec VPN do not have a connector between them.
Name: CorporateAndSecuredCompositeServicesMistmatch (829) Type: serviceAlarm (16) Probable cause: CompositeServiceMisconfiguration (591)	Severity: Warning Object Type (class): IPSecSecuredVpn Domain: ipsec Implicitly cleared (self-clearing): No	The alarm is raised when the corporate and secured services used by an IPsec VPN are in different composite services.
Name: IPSecGatewayDown (830) Type: serviceAlarm (16) Probable cause: gatewayDown (592)	Severity: Major Object Type (class): IPSecGateway Domain: ipsec Implicitly cleared (self-clearing): Yes	The alarm is raised when the Operational State of a SAP IPsec gateway changes to Down and the Administrative State is Up.
Name: IPSecTunnelBfdConnectionBroken (831) Type: serviceAlarm (16) Probable cause: bfdSessionConnectionBroken (593)	Severity: Minor Object Type (class): IPSecTunnelBfd Domain: ipsec Implicitly cleared (self-clearing): Yes	The alarm is raised when the BFD connection to a peer times out.
Name: IPSecTunnelBfdConnectionDown (832) Type: serviceAlarm (16) Probable cause: bfdSessionDown (346)	Severity: Minor Object Type (class): IPSecTunnelBfd Domain: ipsec Implicitly cleared (self-clearing): Yes	The alarm is raised when the Operational State of a BFD session is Not Connected.
Name: IPSecTunnelBfdConnectionPeerDetectsDown (833) Type: serviceAlarm (16) Probable cause: bfdSessionConnectionPeerDetectsDown (594)	Severity: Minor Object Type (class): IPSecTunnelBfd Domain: ipsec Implicitly cleared (self-clearing): Yes	The alarm is raised when a BFD peer detects a connection timeout.
Name: IPSecTunnelDown (834) Type: serviceAlarm (16) Probable cause: tunnelDown (23)	Severity: Major Object Type (class): IPSecTunnel Domain: ipsec Implicitly cleared (self-clearing): Yes	The alarm is raised when the IPsec tunnel Operational State changes to Down and the Administrative State is Up.

Table 3-28 Domain: isa

Alarm	Attributes	Description
Name: IsaAaGrpCapCostThres (835) Type: equipmentAlarm (3) Probable cause: IsaAaGrpCapCostThres (595)	Severity: Warning Object Type (class): AaGroupMember Domain: isa Implicitly cleared (self-clearing): No	The alarm is raised when the capacity cost for an MDA in an ISA-AA group reaches the configured threshold.
Name: IsaAaGrpDown (647) Type: equipmentAlarm (3) Probable cause: IsaAaGrpDown (482)	Severity: Major Object Type (class): AaGroup Domain: isa Implicitly cleared (self-clearing): Yes	The alarm is raised when an ISA-AA group Operational State is Down, and the Administrative State is Up.
Name: IsaAaGrpFailure (564) Type: equipmentAlarm (3) Probable cause: isaAaGrpFailure (434)	Severity: Warning Object Type (class): AaGroup Domain: isa Implicitly cleared (self-clearing): No	The alarm is raised when an ISA-AA Group has no configured primary MDA or the number of active MDAs is not equal to the number of configured primary MDAs.
Name: IsaAaGrpFlowFull (566) Type: equipmentAlarm (3) Probable cause: isaAaGrpFlowFull (436)	Severity: Warning Object Type (class): AaGroup Domain: isa Implicitly cleared (self-clearing): No	The alarm is raised when an ISA-AA group uses a greater number of flow records than the value specified by tmnxBsxFlowFullHighWatermark.
Name: IsaAaGrpNonRedundant (565) Type: equipmentAlarm (3) Probable cause: isaAaGrpNonRedundant (435)	Severity: Warning Object Type (class): AaGroup Domain: isa Implicitly cleared (self-clearing): No	The alarm is raised when an ISA-AA Group has a configured backup MDA but there is no standby MDA available.
Name: IsaAaGrpSwitchover (567) Type: equipmentAlarm (3) Probable cause: isaAaGrpSwitchover (437)	Severity: Warning Object Type (class): AaGroup Domain: isa Implicitly cleared (self-clearing): No	The alarm is raised when an ISA-AA group experiences an activity switch from one ISA-AA to another.
Name: IsaAaSubUnassigned (836) Type: equipmentAlarm (3) Probable cause: IsaAaSubUnassigned (596)	Severity: Warning Object Type (class): AaGroup Domain: isa Implicitly cleared (self-clearing): Yes	The alarm is raised when a subscriber cannot be assigned to an ISA-AA MDA in an AA group because of insufficient service queues, a high AA subscriber count, or a high AA subscriber statistics collection rate. The unassigned subscriber is treated as specified by the Operation Upon Failure parameter in the AA group. Recovery from this condition requires the removal and recreation of the AA subscriber when sufficient resources are available.
Name: IsaLnsGrpDown (1119) Type: equipmentAlarm (3) Probable cause: IsaLnsGrpDown (831)	Severity: Major Object Type (class): LnsGroup Domain: isa Implicitly cleared (self-clearing): Yes	The alarm is raised when the Operational State of an ISA-LNS group is Down and the Administrative State is Up.
Name: IsaVideoGrpDown (775) Type: equipmentAlarm (3) Probable cause: IsaVideoGrpDown (550)	Severity: Major Object Type (class): VideoGroup Domain: isa Implicitly cleared (self-clearing): Yes	The alarm is raised when the Operational State of an ISA video group is Down and the Administrative State is Up.

(1 of 2)

Alarm	Attributes	Description
Name: MgGroupDown (837) Type: MgGroupAlarm (75) Probable cause: MgGroupDown (597)	Severity: Major Object Type (class): MgIsaGroup Domain: isa Implicitly cleared (self-clearing): Yes	The alarm is raised when an MG group goes down.

(2 of 2)

Table 3-29 Domain: isis

Alarm	Attributes	Description
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm (31) Probable cause: IsisInterfaceDown (232)	Severity: Minor Object Type (class): Interface Domain: isis Implicitly cleared (self-clearing): Yes	The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.
Name: IsisAreaMismatch (156) Type: configurationAlarm (11) Probable cause: areaTypeMisconfigured (34)	Severity: Warning Object Type (class): Site Domain: isis Implicitly cleared (self-clearing): Yes	The alarm is raised when IS-IS receives a Hello PDU from an IS with which it does not share an area address.
Name: IsisAuthFailure (155) Type: authenticationAlarm (14) Probable cause: authFailure (46)	Severity: Warning Object Type (class): Site Domain: isis Implicitly cleared (self-clearing): No	The alarm is raised when IS-IS receives a PDU that contains incorrect authentication information.
Name: IsisAuthTypeFailure (154) Type: authenticationAlarm (14) Probable cause: authFailure (46)	Severity: Warning Object Type (class): Site Domain: isis Implicitly cleared (self-clearing): Yes	The alarm is raised when IS-IS receives a PDU that contains the wrong authentication type.
Name: IsisDown (19) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): Site Domain: isis Implicitly cleared (self-clearing): Yes	The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.
Name: IsisExportLimitDropped (838) Type: configurationAlarm (11) Probable cause: exportLimitDropped (598)	Severity: Warning Object Type (class): Site Domain: isis Implicitly cleared (self-clearing): No	The alarm is raised when the number of routes exported from the route table to an IS-IS level drops below the Export Limit value for the level.
Name: IsisExportLimitReached (839) Type: configurationAlarm (11) Probable cause: exportLimitReached (599)	Severity: Warning Object Type (class): Site Domain: isis Implicitly cleared (self-clearing): No	The alarm is raised when the number of routes exported from the route table to an IS-IS level is equal to the Export Limit value for the level.
Name: IsisExportLimitWarning (840) Type: configurationAlarm (11) Probable cause: exportLimitWarning (600)	Severity: Warning Object Type (class): Site Domain: isis Implicitly cleared (self-clearing): No	The alarm is raised when the number of routes exported from the route table to an IS-IS level is equal to the Export Limit percentage specified by the Export Limit Log Percent value.
Name: IsisInterfaceDown (301) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Warning Object Type (class): Interface Domain: isis Implicitly cleared (self-clearing): Yes	The alarm is raised when an IS-IS interface has an Operational State other than Up.

(1 of 2)

Alarm	Attributes	Description
Name: IsisManualAddressDrops (157) Type: configurationAlarm (11) Probable cause: noError (44)	Severity: Warning Object Type (class): Site Domain: isis Implicitly cleared (self-clearing): No	The alarm is raised when a manual area address assigned to an IS is ignored during a route computation.
Name: IsisRejectedAdjacency (214) Type: adjacencyAlarm (31) Probable cause: interfaceMismatch (170)	Severity: Minor Object Type (class): Interface Domain: isis Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM receives a vRtrIsisRejectedAdjacency trap, which indicates that an adjacency cannot be established in response to a Hello PDU from an IS because of a lack of resources.

(2 of 2)

Table 3-30 Domain: l2fwd

Alarm	Attributes	Description
Name: CircuitStpExceptionCondition (648) Type: SdpBindingAlarm (30) Probable cause: StpException (228)	Severity: Major Object Type (class): CircuitStp Domain: l2fwd Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE detects an STP exception condition on a SAP, for example, one-way communication or a downstream loop. The alarm clears when the STP status changes.
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm (28) Probable cause: resourceLimitReached (131)	Severity: Major Object Type (class): SiteFib Domain: l2fwd Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.
Name: MissingLocalEntry (291) Type: configurationAlarm (11) Probable cause: Protected_Mac_Address_Not_Global (222)	Severity: Minor Object Type (class): ServiceMacProtection Domain: l2fwd Implicitly cleared (self-clearing): Yes	The alarm is raised when a protected MAC address that is distributed to all sites in a VPLS is removed from a site using CLI.
Name: MrpAttrTblSizeLimitReached (574) Type: resourceAlarm (28) Probable cause: resourceLimitReached (131)	Severity: Major Object Type (class): SiteMrp Domain: l2fwd Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of MRP attribute table entries for a service site exceeds the high watermark specified by l2fwd.SiteMrp.mrpAttrTblHighWatermark. The alarm clears when the number of MRP attribute table entries for the site drops below the low watermark specified by l2fwd.SiteMrp.mrpAttrTblLowWatermark.

(1 of 2)

Alarm	Attributes	Description
Name: ReceivedHigherBridgePriority (504) Type: SdpBindingAlarm (30) Probable cause: customerDeviceMisconfigured (332)	Severity: Warning Object Type (class): CircuitStp Domain: l2fwd Implicitly cleared (self-clearing): No	The alarm is raised when a customer NE is configured with a bridge priority of zero. The SDP binding that connects to the customer device is subsequently blocked.
Name: sapReceivedProtSrcMac (393) Type: accessInterfaceAlarm (40) Probable cause: ProtectedSourceMacLearned (294)	Severity: Minor Object Type (class): AccessInterfaceFib Domain: l2fwd Implicitly cleared (self-clearing): No	The alarm is raised when a a restricted SAP receives a relearn request for a protected MAC address.
Name: StpExceptionCondition (297) Type: AccessInterfaceAlarm (32) Probable cause: StpException (228)	Severity: Major Object Type (class): AccessInterfaceStp Domain: l2fwd Implicitly cleared (self-clearing): Yes	The alarm is raised when a SAP detects an STP exception condition, for example, one-way communication or a downstream loop. The alarm clears when the STP condition changes.
Name: StpRootGuardViolation (503) Type: AccessInterfaceAlarm (32) Probable cause: spanningTreeTopologyChanged (331)	Severity: Warning Object Type (class): AccessInterfaceStp Domain: l2fwd Implicitly cleared (self-clearing): Yes	The alarm is raised when a SAP detects an STP root guard violation.

(2 of 2)

Table 3-31 Domain: l2tp

Alarm	Attributes	Description
Name: L2TPDown (841) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): Site Domain: l2tp Implicitly cleared (self-clearing): Yes	The alarm is raised when an L2TP site becomes administratively down. The alarm clears when the L2TP site becomes administratively up.
Name: PeerUnreachable (842) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): Peer Domain: l2tp Implicitly cleared (self-clearing): Yes	The alarm is raised when an L2TP peer becomes unreachable.

Table 3-32 Domain: l3fwd

Alarm	Attributes	Description
Name: DuplicateVrfPolicy (229) Type: configurationAlarm (11) Probable cause: duplicateVrfPolicyExists (177)	Severity: Warning Object Type (class): ServiceSiteExportPolicy, ServiceSiteImportPolicy Domain: l3fwd Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects a duplicate VRF policy in a VPRN. The alarm information includes the VRF policy ID and type, and information about the service site.

(1 of 3)

Alarm	Attributes	Description
Name: DuplicateVrfTarget (230) Type: configurationAlarm (11) Probable cause: duplicateVrfTargetExists (178)	Severity: Warning Object Type (class): ServiceSite Domain: l3fwd Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects a duplicate VRF target in a VPRN. The alarm information includes the VRF policy ID and type, and information about the service site.
Name: ExportPolicyNotFound (231) Type: configurationAlarm (11) Probable cause: exportPolicyDoesNotExist (179)	Severity: Major Object Type (class): ServiceSiteExportPolicy Domain: l3fwd Implicitly cleared (self-clearing): Yes	The alarm is raised when a VRF export policy for a VPRN cannot be found. The alarm information includes the policy ID.
Name: HighLevelRoutesReached (1197) Type: ProtocolAlarm (1) Probable cause: HighLevelRoutesReached (897)	Severity: Minor Object Type (class): ServiceSite Domain: l3fwd Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of routes in a VPRN exceeds the high threshold value.The high threshold value is a percentage of the maximum number of routes specified in the VPRN configuration.The percentage is derived by adding 100 to the threshold value in the VPRN configuration and dividing the result by 2.The alarm information includes the number of routes and this calculated high threshold value.
Name: ImportPolicyNotFound (232) Type: configurationAlarm (11) Probable cause: importPolicyDoesNotExist (180)	Severity: Major Object Type (class): ServiceSiteImportPolicy Domain: l3fwd Implicitly cleared (self-clearing): Yes	The alarm is raised when a VRF import policy for a VPRN cannot be found. The alarm information includes the policy ID.
Name: MaxNumIpv6RoutesReached (505) Type: ProtocolAlarm (1) Probable cause: MaxNumIpv6RouteReached (389)	Severity: Major Object Type (class): ServiceSite Domain: l3fwd Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of IPv6 routes in a VPRN exceeds the configured maximum.
Name: MaxNumMcastRoutes (206) Type: ProtocolAlarm (1) Probable cause: MaxNumMcastRoutesReached (160)	Severity: Major Object Type (class): Site Domain: l3fwd Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of multicast routes in a VPRN exceeds the configured maximum.
Name: MaxNumRoutesReached (1198) Type: ProtocolAlarm (1) Probable cause: MaxNumRoutesReached (898)	Severity: Major Object Type (class): ServiceSite Domain: l3fwd Implicitly cleared (self-clearing): No	The alarm is raised when the number of routes in a VPRN reaches the maximum number of routes specified in the VPRN configuration.The alarm information includes the number of routes, the specified maximum, and the route type, which is either IPv4 or IPv6.
Name: McastRoutesMidLevelThresholdReached (207) Type: ProtocolAlarm (1) Probable cause: MidLevelThresholdReached (161)	Severity: Minor Object Type (class): Site Domain: l3fwd Implicitly cleared (self-clearing): No	The alarm is raised when the number of multicast routes in a VPRN exceeds the configured threshold value. The alarm information includes the number of multicast routes and the threshold value.

(2 of 3)

Alarm	Attributes	Description
Name: MidLevelIPv6RoutesReached (506) Type: ProtocolAlarm (1) Probable cause: MidLevelIPv6RoutesReached (390)	Severity: Minor Object Type (class): ServiceSite Domain: l3fwd Implicitly cleared (self-clearing): No	The alarm is raised when the number of IPv6 routes in a VPRN exceeds the configured threshold value. The alarm information includes the number of IPv6 routes and the threshold value.
Name: MidLevelRoutesReached (1199) Type: ProtocolAlarm (1) Probable cause: MidLevelRoutesReached (899)	Severity: Minor Object Type (class): ServiceSite Domain: l3fwd Implicitly cleared (self-clearing): No	The alarm is raised when the number of routes in a VPRN exceeds the threshold specified in the VPRN configuration.The threshold value is a percentage of the maximum number of routes specified in the VPRN configuration.The alarm information includes the number of routes and the threshold value.
Name: MVPNDuplicateVrfPolicy (649) Type: configurationAlarm (11) Probable cause: duplicateVrfPolicyExists (177)	Severity: Warning Object Type (class): ServiceSiteMVPNExportPolicy, ServiceSiteMVPNImportPolicy Domain: l3fwd Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects a duplicate VRF policy in a multicast VPRN. The alarm information includes the VRF policy ID and type, and information about the service site.
Name: MVPNExportPolicyNotFound (650) Type: configurationAlarm (11) Probable cause: exportPolicyDoesNotExist (179)	Severity: Major Object Type (class): ServiceSiteMVPNExportPolicy Domain: l3fwd Implicitly cleared (self-clearing): Yes	The alarm is raised when a VRF export policy for a multicast VPRN cannot be found. The alarm information includes the policy ID.
Name: MVPNImportPolicyNotFound (651) Type: configurationAlarm (11) Probable cause: importPolicyDoesNotExist (180)	Severity: Major Object Type (class): ServiceSiteMVPNImportPolicy Domain: l3fwd Implicitly cleared (self-clearing): Yes	The alarm is raised when a VRF import policy for a multicast VPRN cannot be found. The alarm information includes the policy ID.
Name: RouteDistinguisherNotConfigured (142) Type: configurationAlarm (11) Probable cause: routeDistinguisherNotConfigured (113)	Severity: Major Object Type (class): ServiceSite Domain: l3fwd Implicitly cleared (self-clearing): Yes	The alarm is raised when no RD is configured for an L3 service site.
Name: SingleSFMOverloadDetected (843) Type: ProtocolAlarm (1) Probable cause: signleSfmOverloadDetected (601)	Severity: Major Object Type (class): Site Domain: l3fwd Implicitly cleared (self-clearing): Yes	The alarm is raised when a device reports a single-SFM overload. The alarm clears when the VR exits the Overload state.

(3 of 3)

Table 3-33 Domain: lag

Alarm	Attributes	Description
Name: AsymmetricalConfig (295) Type: configurationAlarm (11) Probable cause: asymmetricalConfig (226)	Severity: Major Object Type (class): MultiChassisLag, MultiChassisLagMember Domain: lag Implicitly cleared (self-clearing): Yes	The alarm is raised when the members of an MC LAG do not have matching configurations.

(1 of 2)

Alarm	Attributes	Description
Name: IncompleteConfig (294) Type: configurationAlarm (11) Probable cause: incompleteConfig (225)	Severity: Major Object Type (class): MultiChassisLag Domain: lag Implicitly cleared (self-clearing): Yes	The alarm is raised when an MC LAG has fewer than two members.
Name: LagDown (20) Type: equipmentAlarm (3) Probable cause: lagDown (17)	Severity: Critical Object Type (class): Interface Domain: lag Implicitly cleared (self-clearing): Yes	The alarm is raised when all ports in a LAG are operationally down.
Name: LinkAggMemberMisconfigured (652) Type: lnkaggAlarm (56) Probable cause: lagMemberMisconfigured (483)	Severity: Critical Object Type (class): Interface Domain: lag Implicitly cleared (self-clearing): Yes	The alarm is raised when one or more misconfigured LAG members are detected, for example, when some LAG members are in access mode and some are in network mode.
Name: LinkAggModeMisconfigured (653) Type: lnkaggAlarm (56) Probable cause: lagModeMisconfigured (484)	Severity: Critical Object Type (class): Interface Domain: lag Implicitly cleared (self-clearing): Yes	The alarm is raised when the LAG mode differs from the mode of one or more LAG members, for example, when the LAG mode is access and the LAG members are in network mode.
Name: LinkAggPortJoin (654) Type: lnkaggAlarm (56) Probable cause: lagPortJoin (485)	Severity: Info Object Type (class): Interface Domain: lag Implicitly cleared (self-clearing): No	The alarm is raised when a LAG port joins a LAG by entering the attached state.
Name: LinkAggPortLeave (655) Type: lnkaggAlarm (56) Probable cause: lagPortLeave (486)	Severity: Info Object Type (class): Interface Domain: lag Implicitly cleared (self-clearing): No	The alarm is raised when a LAG port leaves a LAG by exiting the attached state.
Name: LinkAggPortRemove (656) Type: lnkaggAlarm (56) Probable cause: lagPortRemove (487)	Severity: Warning Object Type (class): Interface Domain: lag Implicitly cleared (self-clearing): No	The alarm is raised when a LAG port is removed from a LAG because of an invalid configuration.
Name: MCLagDown (394) Type: equipmentAlarm (3) Probable cause: mcLagDown (295)	Severity: Critical Object Type (class): MultiChassisLagSpecifics Domain: lag Implicitly cleared (self-clearing): Yes	The alarm is raised when all ports in an MC LAG are operationally down.
Name: McLagSourceBMacLsbMisconfigured (776) Type: configurationAlarm (11) Probable cause: McLagSourceBMacLsbMisconfigured (551)	Severity: Major Object Type (class): MultiChassisLag Domain: lag Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects a mismatch in the last 16 bits of the source backbone MAC address on the peer device.This mismatch prevents PBB access dual homing from operating.

(2 of 2)

Table 3-34 Domain: layer2

Alarm	Attributes	Description
Name: IgmpSnoopingDown (161) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Warning Object Type (class): Bridge Domain: layer2 Implicitly cleared (self-clearing): Yes	The alarm is raised when IGMP snooping is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.
Name: MvrSiteDown (162) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Warning Object Type (class): MvrSite Domain: layer2 Implicitly cleared (self-clearing): Yes	The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.
Name: TlsSiteDown (163) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Warning Object Type (class): TlsSite Domain: layer2 Implicitly cleared (self-clearing): Yes	The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.

Table 3-35 Domain: ldp

Alarm	Attributes	Description
Name: LdpDown (22) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): Site Domain: ldp Implicitly cleared (self-clearing): Yes	The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.
Name: LdpInterfaceDown (21) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): Interface Domain: ldp Implicitly cleared (self-clearing): No	The alarm is raised when an LDP interface is operationally down.
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): TargetedPeer Domain: ldp Implicitly cleared (self-clearing): Yes	The alarm is raised when an LDP targeted peer is operationally down.
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm (18) Probable cause: networkDegradation (204)	Severity: Major Object Type (class): Site Domain: ldp Implicitly cleared (self-clearing): Yes	The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.

Table 3-36 Domain: lps

Alarm	Attributes	Description
Name: LpsLearnMac (519) Type: learnedPortSecurityAlarm (51) Probable cause: portLearnedBridgedMAC (394)	Severity: Warning Object Type (class): LearnedPortSecurity Domain: lps Implicitly cleared (self-clearing): Yes	The alarm is raised when an LPS port learns a bridged MAC address.
Name: LpsPortUpAfterLearningWindowExpired (517) Type: learnedPortSecurityAlarm (51) Probable cause: portUpAfterLearningWindowExpired (392)	Severity: Warning Object Type (class): LPSConfiguration Domain: lps Implicitly cleared (self-clearing): Yes	The alarm is raised in the following situations:- when an LPS port joins or is enabled after the learning window expires and MAC address learning on the port is disabled- when the learning window expires with slice and port values of 0
Name: LpsViolation (518) Type: learnedPortSecurityAlarm (51) Probable cause: learnedPortSecurityViolation (393)	Severity: Major Object Type (class): LearnedPortSecurity Domain: lps Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects an LPS violation.

Table 3-37 Domain: mediation

Alarm	Attributes	Description
Name: CorruptImageFile (171) Type: configurationAlarm (11) Probable cause: invalidOrCorruptImageFile (134)	Severity: Critical Object Type (class): AbstractSoftwareFolderDescriptor Domain: mediation Implicitly cleared (self-clearing): Yes	The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent.The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade.The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.

Table 3-38 Domain: mirror

Alarm	Attributes	Description
Name: MirrorDestinationMisconfigured (209) Type: configurationAlarm (11) Probable cause: mirrorDestinationMisconfigured (162)	Severity: Major Object Type (class): Mirror Domain: mirror Implicitly cleared (self-clearing): Yes	The alarm is raised when multiple destination SAPs are configured for a service mirror.

(1 of 2)

Alarm	Attributes	Description
Name: MirrorEncapsulationTypeInconsistent (217) Type: configurationAlarm (11) Probable cause: mirrorEncapsulationTypeInconsistent (171)	Severity: Major Object Type (class): Mirror Domain: mirror Implicitly cleared (self-clearing): Yes	The alarm is raised when the encapsulation types of the source and destination mirror sites differ.
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm (18) Probable cause: networkDegradation (204)	Severity: Major Object Type (class): Mirror Domain: mirror Implicitly cleared (self-clearing): Yes	The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.

(2 of 2)

Table 3-39 Domain: mirrorli

Alarm	Attributes	Description
Name: liDestinationChangeReject (551) Type: ConfigurationAlarm (15) Probable cause: tMirrorDestinationChangeReject (421)	Severity: Warning Object Type (class): LIMirrorSiteCfg Domain: mirrorli Implicitly cleared (self-clearing): No	The alarm is raised when an operator tries to modify a mirror destination that is in use by an LI mirror.
Name: liDestinationEnabled (550) Type: ConfigurationAlarm (15) Probable cause: tMirrorDestinationEnabled (420)	Severity: Warning Object Type (class): LIMirrorSiteCfg Domain: mirrorli Implicitly cleared (self-clearing): No	The alarm is raised when a mirror destination Operational State changes from Down to Up.
Name: liFilterAssignToItfWarn (556) Type: ConfigurationAlarm (15) Probable cause: tMirrorFilterAssignToItfWarn (426)	Severity: Warning Object Type (class): LIMirrorSiteCfg Domain: mirrorli Implicitly cleared (self-clearing): No	The alarm is raised when an operator tries to assign a filter that is in use by LI to an interface.
Name: liFilterAssignToSapWarn (554) Type: ConfigurationAlarm (15) Probable cause: tMirrorFilterAssignToSapWarn (424)	Severity: Warning Object Type (class): LIMirrorSiteCfg Domain: mirrorli Implicitly cleared (self-clearing): No	The alarm is raised when an operator tries to assign a filter that is in use by LI to a SAP.
Name: liFilterAssignToSdpWarn (555) Type: ConfigurationAlarm (15) Probable cause: tMirrorFilterAssignToSdpWarn (425)	Severity: Warning Object Type (class): LIMirrorSiteCfg Domain: mirrorli Implicitly cleared (self-clearing): No	The alarm is raised when an operator tries to assign a filter that is in use by LI to an SDP.
Name: liSourceDisabled (563) Type: ConfigurationAlarm (15) Probable cause: tMirrorSourceDisabled (433)	Severity: Warning Object Type (class): LISourceCfg Domain: mirrorli Implicitly cleared (self-clearing): No	The alarm is raised when an LI mirror source Operational State changes from Up to Down.
Name: liSourceEnabled (562) Type: ConfigurationAlarm (15) Probable cause: tMirrorSourceEnabled (432)	Severity: Warning Object Type (class): LISourceCfg Domain: mirrorli Implicitly cleared (self-clearing): No	The alarm is raised when an LI mirror source Operational State changes from Down to Up.

(1 of 2)

Alarm	Attributes	Description
Name: liSourceFilterAssignReject (557) Type: ConfigurationAlarm (15) Probable cause: tMirrorSourceFilterAssignReject (427)	Severity: Warning Object Type (class): LIMgmtSite Domain: mirrorli Implicitly cleared (self-clearing): No	The alarm is raised when an operator tries to modify a filter that is in use by LI.
Name: liSourceFilterAssignWarn (559) Type: ConfigurationAlarm (15) Probable cause: tMirrorSourceFilterAssignWarn (429)	Severity: Warning Object Type (class): LIMgmtSite Domain: mirrorli Implicitly cleared (self-clearing): No	The alarm is raised when an operator assigns a mirror filter that is in use by LI and the assignment may be overruled.
Name: liSourceFilterOverruled (558) Type: ConfigurationAlarm (15) Probable cause: tMirrorSourceFilterOverruled (428)	Severity: Warning Object Type (class): LIMgmtSite Domain: mirrorli Implicitly cleared (self-clearing): No	The alarm is raised when the assignment of a mirror filter is overruled by another filter assignment.
Name: liSourceIPFltrChangeReject (552) Type: ConfigurationAlarm (15) Probable cause: tMirrorSourceIPFltrChangeReject (422)	Severity: Warning Object Type (class): LIMirrorSiteCfg Domain: mirrorli Implicitly cleared (self-clearing): No	The alarm is raised when an operator tries to modify an IP filter or an IP filter entry that is in use by LI.
Name: liSourceMacFltrChangeReject (553) Type: ConfigurationAlarm (15) Probable cause: tMirrorSourceMacFltrChangeReject (423)	Severity: Warning Object Type (class): LIMirrorSiteCfg Domain: mirrorli Implicitly cleared (self-clearing): No	The alarm is raised when an operator tries to modify a MAC filter or a MAC filter entry that is in use by LI.
Name: liSourceSapChange (560) Type: ConfigurationAlarm (15) Probable cause: tMirrorSourceSapChange (430)	Severity: Warning Object Type (class): LISourceInterface Domain: mirrorli Implicitly cleared (self-clearing): No	The alarm is raised when a SAP that is associated with LI is modified or deleted.
Name: liSourceSubscriberChange (561) Type: ConfigurationAlarm (15) Probable cause: tMirrorSourceSubChange (431)	Severity: Warning Object Type (class): LISourceSubscriberHost Domain: mirrorli Implicitly cleared (self-clearing): No	The alarm is raised when a subscriber that is associated with LI is modified or deleted.

(2 of 2)

Table 3-40 Domain: mld

Alarm	Attributes	Description
Name: MldDown (587) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): Site Domain: mld Implicitly cleared (self-clearing): Yes	The alarm is raised when an MLD site has an Operational State other than Up, and the Administrative State is Up.

Table 3-41 Domain: mpls

Alarm	Attributes	Description
Name: LastHopIncorrectLabelAction (352) Type: configurationAlarm (11) Probable cause: LabelActionIsNotPopOnLastHop (254)	Severity: Warning Object Type (class): StaticLsp Domain: mpls Implicitly cleared (self-clearing): Yes	The alarm is raised when the label action specified for the last hop in a static LSP is not a pop action.
Name: LastHopNotMatchingDestination (351) Type: configurationAlarm (11) Probable cause: LastHopNotMatchingDestination (253)	Severity: Warning Object Type (class): StaticLsp Domain: mpls Implicitly cleared (self-clearing): Yes	The alarm is raised when the last hop in a static LSP is not the destination.
Name: LspDown (25) Type: pathAlarm (12) Probable cause: lspDown (19)	Severity: Critical Object Type (class): Lsp Domain: mpls Implicitly cleared (self-clearing): Yes	The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.
Name: LspPathBypassTunnelActive (264) Type: pathAlarm (12) Probable cause: LspPathReroutedToBypassTunnel (197)	Severity: Warning Object Type (class): LspPath Domain: mpls Implicitly cleared (self-clearing): Yes	The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.
Name: LspPathDown (26) Type: pathAlarm (12) Probable cause: lspPathDown (20)	Severity: Major Object Type (class): LspPath Domain: mpls Implicitly cleared (self-clearing): Yes	The alarm is raised when an LSP path is operationally down.
Name: MissingHopConfiguration (350) Type: configurationAlarm (11) Probable cause: MissingHopConfiguration (252)	Severity: Warning Object Type (class): StaticLsp Domain: mpls Implicitly cleared (self-clearing): Yes	The alarm is raised when a static LSP is created without hops.
Name: MplsDown (27) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): Site Domain: mpls Implicitly cleared (self-clearing): Yes	The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.
Name: MplsPathUpdateFailed (1066) Type: pathAlarm (12) Probable causes: • mbbRetryExceeded (804) • lspPathGoingDown (805) • startingHighPriMbb (806) • restartingMbb (807) • highPriMbbInProg (808)	Severity: Major Object Type (class): LspPath Domain: mpls Implicitly cleared (self-clearing): Yes	The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.
Name: MplsResignalTimerExpired (1121) Type: ProtocolAlarm (1) Probable cause: resignalTimerExpired (833)	Severity: Info Object Type (class): Site Domain: mpls Implicitly cleared (self-clearing): No	The alarm is raised when an MPLS instance resignal timer expires.

(1 of 2)

Alarm	Attributes	Description
Name: PathReoptimized (28) Type: pathAlarm (12) Probable cause: pathReoptimized (21)	Severity: Warning Object Type (class): Tunnel Domain: mpls Implicitly cleared (self-clearing): No	The alarm is raised when an MPLS path generates an mplsTunnelReoptimized trap.
Name: PathRerouted (29) Type: pathAlarm (12) Probable cause: pathRerouted (22)	Severity: Warning Object Type (class): Tunnel Domain: mpls Implicitly cleared (self-clearing): No	The alarm is raised when an MPLS path generates an mplsTunnelRerouted trap.
Name: S2LPathBypassTunnelActive (777) Type: pathAlarm (12) Probable cause: S2LPathReroutedToBypassTunnel (552)	Severity: Warning Object Type (class): S2LPath Domain: mpls Implicitly cleared (self-clearing): Yes	The alarm is raised when the bypass tunnel in an S2L path becomes active.The alarm clears when the bypass tunnel is no longer active, for example, because a primary tunnel failure is resolved or a new path is established.
Name: S2LPathDown (778) Type: pathAlarm (12) Probable cause: S2LPathDown (553)	Severity: Major Object Type (class): S2LPath Domain: mpls Implicitly cleared (self-clearing): Yes	The alarm is raised when the S2L path Administrative State is Up and the Operational State is not Up.The alarm clears when the S2L path Operational State changes to Up or the Administrative State changes to Down.
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm (18) Probable cause: networkDegradation (204)	Severity: Major Object Type (class): Lsp Domain: mpls Implicitly cleared (self-clearing): Yes	The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.
Name: TestThresholdExceededAlarm2 (1918) Type: oamAlarm (18) Probable cause: networkDegradation (204)	Severity: Major Object Type (class): P2MPDynamicLsp Domain: mpls Implicitly cleared (self-clearing): Yes	The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.
Name: TestThresholdExceededAlarm3 (1919) Type: oamAlarm (18) Probable cause: networkDegradation (204)	Severity: Major Object Type (class): LspPath Domain: mpls Implicitly cleared (self-clearing): Yes	The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.
Name: TunnelAdministrativelyDown (523) Type: pathAlarm (12) Probable cause: tunnelAdministrativelyDown (333)	Severity: Minor Object Type (class): Tunnel Domain: mpls Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.
Name: TunnelDown (30) Type: pathAlarm (12) Probable cause: tunnelDown (23)	Severity: Warning Object Type (class): Tunnel Domain: mpls Implicitly cleared (self-clearing): Yes	The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.

(2 of 2)

Table 3-42 Domain: mpr

Alarm	Attributes	Description
Name: CrossconnectDown (744) Type: CrossconnectAlarm (60) Probable cause: crossconnectDown (520)	Severity: Major Object Type (class): Crossconnect Domain: mpr Implicitly cleared (self-clearing): Yes	The alarm is raised when the Operational State of an L2 or L3 interface is Down, and the Administrative State of the associated site is Up.The alarm is not raised against an L2 access interface that is in the MC ring standby state.
Name: EcIdRxTxOrMacModified (802) Type: configurationAlarm (11) Probable cause: ecIdRxTxOrMacModified (568)	Severity: Minor Object Type (class): MprVll Domain: mpr Implicitly cleared (self-clearing): No	The alarm is raised when something other than the 5620 SAM deletes a service cross-connect and creates a new service cross-connect whose MAC address, EC ID Rx, or EC ID Tx value does not match the value in the original service.
Name: InSufficientBandwidth (745) Type: communicationsAlarm (4) Probable cause: inSufficientBandwidth (521)	Severity: Major Object Type (class): VlanPathInstance Domain: mpr Implicitly cleared (self-clearing): Yes	The alarm is raised when there is insufficient bandwidth on a radio link between hops in a service.
Name: LCD (803) Type: communicationsAlarm (4) Probable cause: lossOfCellDelineation (569)	Severity: Major Object Type (class): IMALink Domain: mpr Implicitly cleared (self-clearing): Yes	The alarm is raised when a Loss of Cell Delineation signal is detected on an ASAP MDA.
Name: LIF (804) Type: communicationsAlarm (4) Probable cause: lossOfIMAFrame (570)	Severity: Major Object Type (class): IMALink Domain: mpr Implicitly cleared (self-clearing): Yes	The alarm is raised when a Loss of IMA Frame signal is detected on an ASAP MDA.
Name: LODS (805) Type: communicationsAlarm (4) Probable cause: lossOfDelaySynchronization (571)	Severity: Major Object Type (class): IMALink Domain: mpr Implicitly cleared (self-clearing): Yes	The alarm is raised when a Loss of Delay Sychronization signal is detected on an ASAP MDA.
Name: MisconfiguredInflow (1067) Type: communicationsAlarm (4) Probable cause: misconfiguredInflow (809)	Severity: Major Object Type (class): VlanPathInstance Domain: mpr Implicitly cleared (self-clearing): Yes	The alarm is raised when the ports in a service use different inflow clock sources.
Name: MprVllDown (1139) Type: serviceDown (88) Probable cause: vlanPathInstanceDown (524)	Severity: Major Object Type (class): MprVll Domain: mpr Implicitly cleared (self-clearing): Yes	The alarm is raised when the Operational State of a VLAN path instance is Down, for example, because of one of the following conditions:- The radio link is down.- A cross connect is deleted.- The Operational State of one or more ports in the cross connect is Down.
Name: PhysicalLinkDown (1140) Type: communicationsAlarm (4) Probable cause: PhysicalLinkDown (846)	Severity: Major Object Type (class): VlanPath Domain: mpr Implicitly cleared (self-clearing): Yes	The alarm is raised when the radio link between two hops of a VLAN path is down.

(1 of 2)

Alarm	Attributes	Description
Name: PortsSeggregated (746) Type: communicationsAlarm (4) Probable cause: portsSeggregated (522)	Severity: Major Object Type (class): VlanPathInstance Domain: mpr Implicitly cleared (self-clearing): Yes	The alarm is raised when the two ports that are to be part of a service cross-connect are segregated.
Name: RadioLinkDown (747) Type: communicationsAlarm (4) Probable cause: radioLinkDown (523)	Severity: Major Object Type (class): VlanPath Domain: mpr Implicitly cleared (self-clearing): Yes	The alarm is raised when the radio link between two hops of a VLAN path is down.
Name: RDI (806) Type: communicationsAlarm (4) Probable cause: remoteDefectIndication (572)	Severity: Minor Object Type (class): IMALink Domain: mpr Implicitly cleared (self-clearing): Yes	The alarm is raised when a Remote Defect Indication signal is detected on an ASAP MDA.
Name: TMNLossofSignal (1920) Type: communicationsAlarm (4) Probable cause: tmnLOS (920)	Severity: Major Object Type (class): MprTMN Domain: mpr Implicitly cleared (self-clearing): Yes	This is raised when Loss of Signal occurs on the TMN Interface.
Name: VlanPathInstanceDown (748) Type: VlanPathInstanceAlarm (61) Probable cause: vlanPathInstanceDown (524)	Severity: Major Object Type (class): VlanPathInstance Domain: mpr Implicitly cleared (self-clearing): Yes	The alarm is raised when the Operational State of a VLAN path instance is Down, for example, because of one of the following conditions:- The radio link is down.- A cross connect is deleted.- The Operational State of one or more ports in the cross connect is Down.

(2 of 2)

Table 3-43 Domain: msdp

Alarm	Attributes	Description
Name: MsdpActSrcLimExcd (380) Type: communicationsAlarm (4) Probable cause: MsdpActiveSourcesLimitExceeded (279)	Severity: Warning Object Type (class): Site Domain: msdp Implicitly cleared (self-clearing): No	The alarm is raised when an MSDP site receives a number of source active messages that exceeds the configured maximum.
Name: MsdpDown (353) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): Site Domain: msdp Implicitly cleared (self-clearing): Yes	The alarm is raised when an MSDP site is administratively down. The alarm clears when the site is administratively up.
Name: MsdpGroupSrcActMsgsExcd (378) Type: communicationsAlarm (4) Probable cause: MsdpGroupActiveSourcesLimitExceeded (277)	Severity: Warning Object Type (class): PeerGroup Domain: msdp Implicitly cleared (self-clearing): No	The alarm is raised when an MSDP group receives a number of source active messages that exceeds the configured maximum.
Name: MsdpPeerActSrcLimExcd (379) Type: communicationsAlarm (4) Probable cause: MsdpPeerActiveSourcesLimitExceeded (278)	Severity: Warning Object Type (class): GroupPeer, Peer Domain: msdp Implicitly cleared (self-clearing): No	The alarm is raised when an MSDP peer receives a number of source active messages that exceeds the configured maximum.

(1 of 2)

Alarm	Attributes	Description
Name: MsdpRPFFailure (354) Type: communicationsAlarm (4) Probable cause: MsdpRPFFailure (275)	Severity: Warning Object Type (class): Site Domain: msdp Implicitly cleared (self-clearing): No	The alarm is raised when an MSDP site experiences an RPF failure.
Name: MsdpSourceSrcActMsgsExcd (381) Type: communicationsAlarm (4) Probable cause: MsdpSourceActiveSourcesLimitExceeded (280)	Severity: Warning Object Type (class): Source Domain: msdp Implicitly cleared (self-clearing): No	The alarm is raised when an MSDP source receives a number of source active messages that exceeds the configured maximum.
Name: PeerConnectionDown (2) Type: ProtocolAlarm (1) Probable cause: connectionDown (2)	Severity: Critical Object Type (class): CommonPeer Domain: msdp Implicitly cleared (self-clearing): Yes	The alarm is raised when the connectionState of this peer changes from Established to a state other than Established. The alarm clears when the connectionState of this peer returns to the Established state.
Name: PeerDown (1) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): CommonPeer Domain: msdp Implicitly cleared (self-clearing): Yes	The alarm is raised when the Administrative State of a peer changes from Up to Down. The alarm clears when the Administrative State returns to Up.
Name: PeerGroupDown (5) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): PeerGroup Domain: msdp Implicitly cleared (self-clearing): Yes	The alarm is raised when the Administrative State of a peer group changes from Up to Down. The alarm clears when the Administrative State returns to Up.

(2 of 2)

Table 3-44 Domain: multichassis

Alarm	Attributes	Description
Name: AsymmetricalConfig (295) Type: configurationAlarm (11) Probable cause: asymmetricalConfig (226)	Severity: Major Object Type (class): MultiChassisLag, MultiChassisLagMember, MultiChassisPeer Domain: multichassis Implicitly cleared (self-clearing): Yes	The alarm is raised when there is a peer configuration mismatch that prevents MC operation.
Name: IncompleteConfig (294) Type: configurationAlarm (11) Probable cause: incompleteConfig (225)	Severity: Major Object Type (class): MultiChassisLagMember, MultiChassisSync Domain: multichassis Implicitly cleared (self-clearing): Yes	The alarm is raised when a peer configuration cannot be found on the peer NE.
Name: IncorrectEndPointPeerConfig (1068) Type: configurationAlarm (11) Probable cause: incompleteEPPeerConfig (810)	Severity: Major Object Type (class): MultiChassisEndpoint Domain: multichassis Implicitly cleared (self-clearing): Yes	The alarm is raised when a peer configuration cannot be found on the peer NE.

(1 of 3)

Alarm	Attributes	Description
Name: IncorrectPeerConfig (779) Type: configurationAlarm (11) Probable cause: IncorrectPeerConfig (554)	Severity: Major Object Type (class): Peer Domain: multichassis Implicitly cleared (self-clearing): Yes	The alarm is raised when an MC peer does not exist, or when an MC peer exists but the peer address is not the address of a network interface on the peer.
Name: IncorrectPeerSynchronizationPortConfig (780) Type: configurationAlarm (11) Probable cause: IncorrectPeerSynchronizationPortConfig (555)	Severity: Major Object Type (class): PeerSynchronizationPort Domain: multichassis Implicitly cleared (self-clearing): Yes	The alarm is raised when the peer port does not exist, or when the peer port exists but the synchronization tags of the peers do not match.
Name: IncorrectPeerSynchronizationPortEncapRangeConfig (781) Type: configurationAlarm (11) Probable cause: IncorrectPeerSynchronizationPortEncapRangeConfig (556)	Severity: Major Object Type (class): PeerSynchronizationPortEncapRange Domain: multichassis Implicitly cleared (self-clearing): Yes	The alarm is raised when an MC synchronization group does not have a configured VLAN range, or when the VLAN ranges on the MC synchronization peers do not match.
Name: LocalRncvOperDown (521) Type: redundancyAlarm (52) Probable cause: localRncvDisconnected (396)	Severity: Major Object Type (class): MultiChassisRingNode Domain: multichassis Implicitly cleared (self-clearing): Yes	The alarm is raised when the local RNCV Operational State of a ring node is other than Connected or NotTested, which means that the ring node is not connected to the local MC ring group. The alarm clears when the ring node enters the Connected or NotTested state.
Name: MCLagDown (394) Type: equipmentAlarm (3) Probable cause: mcLagDown (295)	Severity: Critical Object Type (class): MultiChassisLagPeerSpecifics Domain: multichassis Implicitly cleared (self-clearing): Yes	The alarm is raised when all ports in an MC LAG are operationally Down.
Name: McLagSourceBMacLsbMisconfigured (776) Type: configurationAlarm (11) Probable cause: McLagSourceBMacLsbMisconfigured (551)	Severity: Major Object Type (class): MultiChassisLag Domain: multichassis Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects a mismatch in the last 16 bits of the source backbone MAC address on the peer device.This mismatch prevents PBB access dual homing from operating.
Name: MCPeerEPDown (1069) Type: equipmentAlarm (3) Probable cause: MCPeerEPDown (811)	Severity: Critical Object Type (class): MultiChassisEndpoint Domain: multichassis Implicitly cleared (self-clearing): Yes	The alarm is raised when an MC endpoint is operationally down.
Name: MultiChassisRingDown (520) Type: redundancyAlarm (52) Probable cause: ringDown (395)	Severity: Major Object Type (class): MultiChassisRing Domain: multichassis Implicitly cleared (self-clearing): Yes	The alarm is raised when a MC ring group Operational State is not in the Connected state. The alarm is cleared when the ring group enters the Connected state.
Name: NoPeerMcRingFound (782) Type: configurationAlarm (11) Probable cause: IncompleteConfig (557)	Severity: Major Object Type (class): MultiChassisRing Domain: multichassis Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM cannot find the peer MC ring.

(2 of 3)

Alarm	Attributes	Description
Name: RemoteRncvOperDown (522) Type: redundancyAlarm (52) Probable cause: remoteRncvDisconnected (397)	Severity: Major Object Type (class): MultiChassisRingNode Domain: multichassis Implicitly cleared (self-clearing): Yes	The alarm is raised when the remote RNCV Operational State of a ring node is other than Connected or NotTested, which means that the ring node is not connected to the local MC ring group. The alarm clears when the ring node enters the Connected or NotTested state.
Name: tmnxMcSyncClientAlarm (423) Type: communicationsAlarm (4) Probable cause: locallyDeletedEntryInMCSyncDatabase (407)	Severity: Warning Object Type (class): PeerSynchronizationProtocol Domain: multichassis Implicitly cleared (self-clearing): Yes	The alarm is raised when a MC synchronization database entry is deleted locally.

(3 of 3)

Table 3-45 Domain: nat

Alarm	Attributes	Description
Name: NatIsaMemberSessionUsageHigh (1070) Type: equipmentAlarm (3) Probable cause: resourceFull (53)	Severity: Major Object Type (class): IsaMda Domain: nat Implicitly cleared (self-clearing): Yes	The alarm is raised when the session usage of an ISA-NAT group member reaches the highwatermark. The alarm clears when the session usage reaches the low watermark.
Name: NatLsnSubIcmpPortUsageHigh (1071) Type: equipmentAlarm (3) Probable cause: resourceFull (53)	Severity: Major Object Type (class): LsnSubscriber Domain: nat Implicitly cleared (self-clearing): Yes	The alarm is raised when the ICMP port usage of a large-scale NAT subscriber reaches the high orlow watermark.
Name: NatLsnSubTcpPortUsageHigh (1072) Type: equipmentAlarm (3) Probable cause: resourceFull (53)	Severity: Major Object Type (class): LsnSubscriber Domain: nat Implicitly cleared (self-clearing): Yes	The alarm is raised when the TCP port usage of a large-scale NAT subscriber reaches the high orlow watermark.
Name: NatLsnSubUdpPortUsageHigh (1073) Type: equipmentAlarm (3) Probable cause: resourceFull (53)	Severity: Major Object Type (class): LsnSubscriber Domain: nat Implicitly cleared (self-clearing): Yes	The alarm is raised when the UDP port usage of a large-scale NAT subscriber reaches the high orlow watermark.
Name: NatPlL2AwBlockUsageHigh (1074) Type: equipmentAlarm (3) Probable cause: resourceFull (53)	Severity: Major Object Type (class): NatPool Domain: nat Implicitly cleared (self-clearing): Yes	The alarm is raised when the block usage of an L2-aware NAT address pool reaches the highwatermark. The alarm clears when the block usage reaches the low watermark.
Name: NatPlLsnMemberBlockUsageHigh (1075) Type: equipmentAlarm (3) Probable cause: resourceFull (53)	Severity: Major Object Type (class): NatPool Domain: nat Implicitly cleared (self-clearing): Yes	The alarm is raised when the block usage of a large-scale NAT address pool reaches the highwatermark. The alarm clears when the block usage reaches the low watermark.

Table 3-46 Domain: netw

Alarm	Attributes	Description
Name: ActivitySwitch (182) Type: communicationsAlarm (4) Probable cause: systemFailed (144)	Severity: Critical Object Type (class): NmsSystem Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when a 5620 SAM main server activity switch occurs.
Name: BootConfigFailScriptNotAccesible (543) Type: configurationAlarm (11) Probable cause: bootConfigFailScriptNotAccesible (416)	Severity: Major Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when a CLI script that runs after NEconfigurationfile execution failure is inaccessible.
Name: BootConfigOKScriptNotAccesible (544) Type: configurationAlarm (11) Probable cause: bootConfigOKScriptNotAccesible (417)	Severity: Major Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when a CLI script that runs after NEconfigurationfile execution success is inaccessible.
Name: BootParametersMisconfigured (35) Type: configurationAlarm (11) Probable causes: • persistentIndexFailure (30) • configFileBootFailure (31)	Severity: Critical Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when the SNMP Index BootStatus on an NE is not setto Persistent.
Name: CliCommandFailure (402) Type: communicationsAlarm (4) Probable cause: cliCommandFailure (300)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when a CLI command on an NEfails.
Name: CliConnectionProblem (299) Type: communicationsAlarm (4) Probable cause: cliConnectionProblem (230)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM fails to open a CLI session onanNE because the number of open CLI sessions on the NE isat the maximum.
Name: CliLoginFailed (298) Type: communicationsAlarm (4) Probable cause: cliLoginFailed (229)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when a CLI login attempt fails because of anincorrect user name or password.
Name: CorruptedUdpPacket (1921) Type: communicationsAlarm (4) Probable cause: corruptedPacket (921)	Severity: Variable or indeterminate Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the an UDP packet iscorruptedfor an application.
Name: CpuUtilizationExceeded (358) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the 7250 SAS CPUutilizationexceeds the configured threshold and the NE sends theBATM-SYS-MON-MIB.cpuUtilizationExceeded trap.

(1 of 12)

Alarm	Attributes	Description
Name: DetectedPreProvisionedCantidateNodeHasConfig (1960) Type: communicationsAlarm (4) Probable cause: detectedPreProvisionedCantidateNodeHasConfig (947)	Severity: Critical Object Type (class): DiscoveredNode Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the cantidate node detected for pre-provisioning alreadyhas configuration in it. This configuration in the detected node will get replacedwith the configuration in the matching pre-provisioned node in SAM during theconfiguration deployment stage of self-config.
Name: DiscoveredPhysicalLinkMismatch (657) Type: configurationAlarm (11) Probable cause: endPointUsedByNumerousLinks (488)	Severity: Warning Object Type (class): AbstractPhysicalLink Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when one endpoint of a physical link is used as an endpoint in another physical link.
Name: DuplicatePhysicalLinks (658) Type: configurationAlarm (11) Probable cause: duplicatePhysicalLinkConfigured (489)	Severity: Minor Object Type (class): AbstractPhysicalLink Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when there is more then one physical link configured between two endpoints.
Name: DuplicateRouterIdProblem (411) Type: configurationAlarm (11) Probable cause: duplicateRouterId (168)	Severity: Critical Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM detectsthat the same address isbeing used by multiple NEs. To prevent 5620 SAM databasecorruption, the 5620 SAM does not discover the NE withthe duplicate address.
Name: EventsThrottled (356) Type: communicationsAlarm (4) Probable cause: snmpDaemonOverloaded (141)	Severity: Major Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when an NE throttles eventsbecausethe event rate exceeds the configured maximum.
Name: FailureToSwitchManagementProtocol (1076) Type: communicationsAlarm (4) Probable cause: managementAddressInvalid (812)	Severity: Major Object Type (class): NodeDiscoveryControl Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM cannot switch the management address of an NE from one IP version to another.
Name: FrameSizeProblem (37) Type: configurationAlarm (11) Probable cause: frameSizeProblem (33)	Severity: Critical Object Type (class): StatefullConnectableInterface Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.
Name: FtpClientFailure (357) Type: communicationsAlarm (4) Probable cause: ftpClientFailure (257)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when an NE sendsnotification thatan FTP operation initiated by the FTP client failsbecause of file unavailability, interruption during thefile transfer, or a lack of available storage space.

(2 of 12)

Alarm	Attributes	Description
Name: GneCommunicationAlarm (783) Type: CommunicationAlarm (64) Probable cause: User_Defined (558)	Severity: Variable or indeterminate Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	This user-definable alarm is raised against ageneric NEwhen the 5620 SAM receives a trap from the generic NE that is mapped to the alarm in a generic NE alarmcatalogue. The alarm mapping defines the Probable cause,Severity, and Implicitly cleared values, and optionallycontains an extension that is appended to the Namevalue.
Name: GneEnvironmentalAlarm (784) Type: EnvironmentalAlarm (65) Probable cause: User_Defined (558)	Severity: Variable or indeterminate Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	This user-definable alarm is raised against ageneric NEwhen the 5620 SAM receives a trap from the generic NEthat is mapped to the alarm in a generic NE alarmcatalogue. The alarm mapping defines the Probable cause,Severity, and Implicitly cleared values, and optionallycontains an extension that is appended to the Namevalue.
Name: GneEquipmentAlarm (785) Type: EquipmentAlarm (66) Probable cause: User_Defined (558)	Severity: Variable or indeterminate Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	This user-definable alarm is raised against ageneric NEwhen the 5620 SAM receives a trap from the generic NEthat is mapped to the alarm in a generic NE alarmcatalogue. The alarm mapping defines the Probable cause,Severity, and Implicitly cleared values, and optionallycontains an extension that is appended to the Namevalue.
Name: GneProcessingErrorAlarm (786) Type: ProcessingErrorAlarm (67) Probable cause: User_Defined (558)	Severity: Variable or indeterminate Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	This user-definable alarm is raised against ageneric NEwhen the 5620 SAM receives a trap from the generic NEthat is mapped to the alarm in a generic NE alarmcatalogue. The alarm mapping defines the Probable cause,Severity, and Implicitly cleared values, and optionallycontains an extension that is appended to the Namevalue.
Name: GneQualityOfServiceAlarm (787) Type: QualityOfServiceAlarm (68) Probable cause: User_Defined (558)	Severity: Variable or indeterminate Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	This user-definable alarm is raised against ageneric NEwhen the 5620 SAM receives a trap from the generic NEthat is mapped to the alarm in a generic NE alarmcatalogue. The alarm mapping defines the Probable cause,Severity, and Implicitly cleared values, and optionallycontains an extension that is appended to the Namevalue.
Name: GneServiceAlarm (788) Type: ServiceAlarm (69) Probable cause: User_Defined (558)	Severity: Variable or indeterminate Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	This user-definable alarm is raised against ageneric NEwhen the 5620 SAM receives a trap from the generic NEthat is mapped to the alarm in a generic NE alarmcatalogue. The alarm mapping defines the Probable cause,Severity, and Implicitly cleared values, and optionallycontains an extension that is appended to the Namevalue.

(3 of 12)

Alarm	Attributes	Description
Name: GneSystemAlarm (789) Type: SystemAlarm (70) Probable cause: User_Defined (558)	Severity: Variable or indeterminate Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	This user-definable alarm is raised against ageneric NEwhen the 5620 SAM receives a trap from the generic NEthat is mapped to the alarm in a generic NE alarmcatalogue. The alarm mapping defines the Probable cause,Severity, and Implicitly cleared values, and optionallycontains an extension that is appended to the Namevalue.
Name: GneTransportAlarm (790) Type: TransportAlarm (71) Probable cause: User_Defined (558)	Severity: Variable or indeterminate Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	This user-definable alarm is raised against ageneric NEwhen the 5620 SAM receives a trap from the generic NEthat is mapped to the alarm in a generic NE alarmcatalogue. The alarm mapping defines the Probable cause,Severity, and Implicitly cleared values, and optionallycontains an extension that is appended to the Namevalue.
Name: InBandManagementConnectionDown (139) Type: communicationsAlarm (4) Probable cause: managementConnectionDown (111)	Severity: Critical Object Type (class): NodeDiscoveryControl Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM cannot reach a managed NE using the ping function over an in-band connection.
Name: IncompleteConfiguration (1942) Type: operationalViolation (93) Probable cause: incompleteConfig (225)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when a pre-provisioned NE has no objects configured beneath it.
Name: InconsistenciesOnNode (1077) Type: integrityViolation (85) Probable cause: inconsistenciesOnNode (813)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when a device detects one or more configurationinconsistencies. On a 9500 MPR, this can becaused bycross-connect creation failure during service creation.
Name: InterfaceDown (36) Type: InterfaceAlarm (13) Probable cause: interfaceDown (32)	Severity: Critical Object Type (class): StatefullConnectableInterface Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.
Name: InvalidBOFAddress (1141) Type: communicationsAlarm (4) Probable cause: invalidBOF (847)	Severity: Warning Object Type (class): NodeDiscoveryControl Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised during a network topology rescan in which the 5620 SAM does not find a previously configured NE BOF address, and the Management IP Selection of the NE is set to one of the following:- Out Of Band Preferred- In Band Preferred
Name: JMSServerDown (360) Type: communicationsAlarm (4) Probable cause: systemFailed (144)	Severity: Critical Object Type (class): NmsSystem Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when JMS communication fails.

(4 of 12)

Alarm	Attributes	Description
Name: ManagementInterfaceProtectionSwitch (34) Type: communicationsAlarm (4) Probable causes: • switchToInband (814) • switchToOutband (815)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when an NE has in-band and out-of-band managementinterfaces and switches from one type ofmanagement tothe other.
Name: ManagementIpAddressMismatch (1943) Type: communicationsAlarm (4) Probable cause: mismatchOfManagementIpAddress (931)	Severity: Major Object Type (class): DiscoveredNode Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when the IP address of the shadow network element does not match with theIP address of the discovered NE.
Name: ManagementIPSwitchUnsupported (1078) Type: communicationsAlarm (4) Probable cause: managementAddressInvalid (812)	Severity: Warning Object Type (class): NodeDiscoveryControl Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when an attempt is made to switch the management address of an NE from one IP version to another.
Name: MemoryConsumption (216) Type: communicationsAlarm (4) Probable cause: tooManyTrapsBuffered (173)	Severity: Major Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when one of the followingoccurs.- The number of traps from a particular NE that await processing bythe 5620 SAM surpasses the NE red threshold fortrapmemory management in the 5620 SAM server configuration.- The global number of traps that await processing bythe 5620 SAM surpasses the yellow threshold for trapmemory management in the 5620 SAM server configuration.Caution: Alcatel-Lucent strongly recommends againstmodifying NE trap management threshold values; modifyingthese values can seriously degrade 5620 SAM performance.The alarm clears when one of the following occurs.- The number of traps from the NE that await processing falls belowthe NE red threshold.- The global number of traps that await processing falls below thesystem yellow threshold. The NE isresynchronized onlyif required.
Name: MisconfiguredNode (382) Type: configurationAlarm (11) Probable causes: • persistOff (281) • noSystemAddress (282) • noIpv4Address (816)	Severity: Major Object Type (class): Topology Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM tries to discover an NE that is not properly configured for management, for example, when persistence is set to Off in the NE BOF, or when the NE has no system address.
Name: MissedStatsCollection (355) Type: communicationsAlarm (4) Probable cause: noAuxiliaryServersAvailable (256)	Severity: Critical Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when a 5620 SAM main servercannotcommunicate with any auxiliary server for NE statisticscollection during a statistics poll.

(5 of 12)

Alarm	Attributes	Description
Name: MissingNESelfConfigPolicy (1944) Type: communicationsAlarm (4) Probable cause: noNESelfConfigPolicyFound (932)	Severity: Major Object Type (class): TopologyDiscoveryRule Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when an identifier of a shadow NE matches the identifier of a node beingdiscovered by a scan of this discovery rule, but there is no NE self-config policy for thenode type set in this discovery rule.
Name: MissingPreProvisionedNode (1945) Type: communicationsAlarm (4) Probable cause: noPreProvisionedNodeFound (933)	Severity: Major Object Type (class): DiscoveredNode Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when there is no pre-provisioned NE to be found to associate thediscovered candidate target NE to.
Name: ModuleOutOfMemory (180) Type: equipmentAlarm (3) Probable cause: outOfMemory (142)	Severity: Critical Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the available NE memoryisinsufficient for allocation to a task.
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm (4) Probable cause: neManagementChange (817)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): Yes	This user-defined alarm is raised when the NE configuration is one ofthe following:- The Active Management IP is set to Out Of Band, and the PrimaryRoute Preference is set to In Band.- The Active Management IP is set to In Band, and the Primary RoutePreference is set to Out of Band.
Name: NetworkElementChassisTypeMismatch (1946) Type: communicationsAlarm (4) Probable cause: mismatchOfNetworkElementChassisType (934)	Severity: Major Object Type (class): DiscoveredNode Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when the chassis type of the shadow network element does not match with thechassis type of the discovered NE.
Name: NetworkElementTypeMismatch (1947) Type: communicationsAlarm (4) Probable cause: mismatchOfNetworkElementType (935)	Severity: Major Object Type (class): DiscoveredNode Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when the type of the shadow network element does not match with the typeof the discovered NE.
Name: NetworkElementVersionMismatch (1948) Type: communicationsAlarm (4) Probable cause: mismatchOfNetworkElementVersion (936)	Severity: Major Object Type (class): DiscoveredNode Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when the version of the shadow network element does not match with theversion of the discovered NE.
Name: NodeAlreadyManagedOverAnotherProtocol (1080) Type: discoveryControlAlarm (33) Probable cause: nodeAlreadyDiscovered (818)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM tries to rediscover apreviouslydiscovered NE using a different IP version.
Name: NodeColdStart (172) Type: equipmentAlarm (3) Probable cause: nodeColdStart (135)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM receives a SNMPv2-MIB.coldStarttrap from an NE.

(6 of 12)

Alarm	Attributes	Description
Name: NodeDatabaseCorruptionDetected (1961) Type: communicationsAlarm (4) Probable cause: nodeDatabaseCorrupted (948)	Severity: Critical Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	This alarm is raised when an error in the node causes the node to lose its configurationand come up in an inconsistent/incomplete state. To overcome this it might be necessary toreconfigure the node.
Name: NodeRebooted (32) Type: equipmentAlarm (3) Probable cause: nodeReboot (25)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM detects an NE reboot based onthelatest NE sysUpTime value.
Name: NodeUpgraded (178) Type: configurationAlarm (11) Probable cause: upgradedNodeVersion (140)	Severity: Info Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM detects an NE software versionupgrade.
Name: NodeVersionMismatch (177) Type: configurationAlarm (11) Probable cause: DowngradedNodeVersion (139)	Severity: Critical Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the software version onan NE differs from theversion recorded for the NE in the 5620 SAM database.
Name: OutOfBandManagementConnectionDown (138) Type: communicationsAlarm (4) Probable cause: managementConnectionDown (111)	Severity: Critical Object Type (class): NodeDiscoveryControl Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM cannot reach a managed NE using the ping function over an out-of-band connection.
Name: PatchLevelMismatch (659) Type: softwareAlarm (19) Probable cause: patchLevelMismatch (490)	Severity: Critical Object Type (class): NmsSystem Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM primary main server software patch level does not match the standby main server software patch level.
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm (11) Probable cause: persistentIndexConfigurationMismatch (136)	Severity: Major Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when persistence is set to Off in the NE BOF.
Name: PhysicalLinkPortsMisconfigured (239) Type: configurationAlarm (11) Probable cause: physicalLinkPortsMisconfigured (181)	Severity: Minor Object Type (class): AbstractPhysicalLink Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when there is an MTU size mismatch between a link endpoint and a port. The alarm clears when the MTUs match.
Name: PollDeadlineMissed (240) Type: configurationAlarm (11) Probable cause: tooManyItemsToPoll (183)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when a 5620 SAM server cannot finish browsing astatistics MIB before a polling intervalexpires.

(7 of 12)

Alarm	Attributes	Description
Name: PollerProblem (31) Type: communicationsAlarm (4) Probable cause: resyncFailed (24)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM is unable to poll a networkobject, for example, because of intermittent orno IPconnectivity to an NE, incorrect SNMP securityparameters, or disabled SNMP on the NE.
Name: RamFreeSpaceExceeded (359) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when a 7250 SAS sends theBATM-SYS-MON-MIB.ramFreeSpaceExceeded trap toindicatethat a configurable RAM utilization threshold isreached.
Name: ReconfigFailure (1949) Type: communicationsAlarm (4) Probable cause: failedReconfig (937)	Severity: Critical Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): Yes	This alarm is raised when the reconfig action failed.
Name: RedAlarmThresholdReached (241) Type: communicationsAlarm (4) Probable cause: tooManyAlarms (182)	Severity: Critical Object Type (class): NmsSystem Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the number of outstanding 5620 SAM alarms reaches the critical threshold. When this happens, the 5620 SAM discards alarms to keep the number below the threshold.
Name: RedundancySwitchover (181) Type: equipmentAlarm (3) Probable cause: redundancySwitchover (143)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when a 5620 SAM main serverreceivesa ssiRedSwitchover trap from an NE, which indicates thatthe standby CPM detects an active CPM failure and ispreparing to take over as the new active CPM.
Name: RedundantRadioLink (1081) Type: configurationAlarm (11) Probable cause: redundantRadioLinkConfigured (819)	Severity: Minor Object Type (class): RadioPhysicalLink Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when a radio link is discovered between two nodes when there is already a physical link(s) between the same nodes.
Name: SnmpAuthenticationFailure (176) Type: authenticationAlarm (14) Probable cause: authFailure (46)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when an NE SNMP agent has received an SNMPmessagethat is not properly authenticated. An NE typically doesnot, by default, send the notification that generatesthe alarm; the notification must be manually enabledthrough CLI.
Name: SnmpDaemonProblem (175) Type: communicationsAlarm (4) Probable cause: snmpDaemonError (138)	Severity: Critical Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when one of the followingoccurs:- The 5620 SAM receives an unexpected response to an SNMP request,for example, when a managed NE sends the wrongobject inresponse to an SMNP get or get-next request.- The 5620 SAM receives the TIMETRA-SYSTEM-MIB.tmnxSnmpdError trapfrom a managed NE.

(8 of 12)

Alarm	Attributes	Description
Name: SnmpDown (410) Type: communicationsAlarm (4) Probable cause: snmpDown (306)	Severity: Critical Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the SNMP agent is manually shut down on anNEand the NE sends a trap to indicate this.
Name: SnmpReachabilityProblem (243) Type: communicationsAlarm (4) Probable cause: SnmpReachabilityTestFailed (176)	Severity: Major Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when an SNMP poll of the SysUpTimeAlarm object onan NE fails, for example, because of networkcongestionor because the NE is too busy to respond. The probablecause is an unreachable NE SNMP agent on the NE. Bydefault, the 5620 SAM polls a managed NE every twominutes. If a poll fails, the alarm is raised.The 5620 SAM polls the NE two minutes after the first failure. Ifsuccessive polls fail, the 5620 SAM raises thepollinginterval for the NE by two minutes after each failure toa maximum of 12 min. The polling interval remains at 12min until the 5620 SAM receives a response from the NE.The alarm clears when the 5620 SAM receives a responsefrom the NE, and the 5620 SAM GUI icon that representsthe NE turns from red to green.
Name: SnmpTrapDropped (179) Type: communicationsAlarm (4) Probable cause: snmpDaemonOverloaded (141)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM receives atmnxTrapDropped notification from an NE toindicate thatthe NE has dropped a trap. As a result, the 5620 SAMresynchronizes the table associated with the droppedtrap.
Name: StandbyCPMManagementConnectionDown (140) Type: communicationsAlarm (4) Probable cause: managementConnectionDown (111)	Severity: Critical Object Type (class): NodeDiscoveryControl Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM cannot reach a managed NE using the ping function.
Name: StandbyServerStatus (208) Type: communicationsAlarm (4) Probable cause: systemFailed (144)	Severity: Critical Object Type (class): NmsSystem Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the primary 5620 SAM main server cannot communicate with the 5620 SAM standby main server. The alarm clears when communication between the servers is restored.
Name: StatisticsCollectionThresholdExceeded (524) Type: communicationsAlarm (4) Probable cause: collectionRateGreaterThanConfigured (398)	Severity: Major Object Type (class): NmsSystem Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the accounting statistics collection rate exceeds the retention specifications.

(9 of 12)

Alarm	Attributes	Description
Name: svcFdbMimDestTableFull (588) Type: resourceAlarm (28) Probable cause: resourceLimitReached (131)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of backboneMACaddress indices on an NE reaches the maximum allowedvalue. The alarm clears when the number of backbone MACaddress indices on the NE falls below 95 percent of themaximum allowed value.
Name: SvcNameUpgradeScriptFailed (1082) Type: scriptAlarm (86) Probable causes: • cliConnectionFailed (820) • cliLoginFailed (229) • executionFailed (821)	Severity: Major Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when a generated NE-upgradeCLIscript fails. Typical causes include the following:- invalid CLI login information in the mediation policy- an unreachable NEManual script execution from the NE properties form may provide moreinformation about the failure.
Name: SystemMemoryConsumption (225) Type: communicationsAlarm (4) Probable cause: tooManyTrapsBuffered (173)	Severity: Critical Object Type (class): NmsSystem Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the global number of SNMP traps that await processing by the 5620 SAM surpasses the system red threshold for trap memory management specified in the base configuration of the 5620 SAM server.Caution: Alcatel-Lucent strongly recommends against modifying NE trap management threshold values; modifying these values can seriously degrade 5620 SAM performance.The alarm clears when the number of traps that await processing falls below the system red threshold. The 5620 SAM resynchronizes the NEs, if required.
Name: SystemNameChange (228) Type: equipmentAlarm (3) Probable cause: systemNameChange (174)	Severity: Major Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE undergoes asystem namechange. The alarm information includes the old systemname and the new system name.
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm (18) Probable cause: networkDegradation (204)	Severity: Major Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised whenSasThresholdExceededAlarm israised for any test on this object.
Name: ThresholdCrossingAlarm (14) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Info Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when a value crosses aconfiguredrising or falling threshold. The alarm informationincludes the current threshold value, the defaultthreshold value, and the threshold name.
Name: TraceError (289) Type: equipmentAlarm (3) Probable cause: traceError (221)	Severity: Critical Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when unusual error log tracemessages are generated on an NE. The alarminformationincludes the title of the logged event and messagedetails.

(10 of 12)

Alarm	Attributes	Description
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm (11) Probable causes: • trapDestinationMisconfigured (26) • duplicateTrapLogId (27)	Severity: Major Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when an SNMP trap destination other than the 5620SAM is configured on an NE.
Name: TrapMalformed (135) Type: communicationsAlarm (4) Probable cause: trapSchemaMismatch (108)	Severity: Major Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the number of varbinds in an incoming SNMPtrap is fewer than the number expected.
Name: TrapRateThresholdExceeded (412) Type: communicationsAlarm (4) Probable cause: trapRateGreaterThanConfigured (307)	Severity: Critical Object Type (class): NmsSystem Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the incoming SNMP trap rate is greater than the configured trap rate threshold.
Name: TrapReceivingFailure (1083) Type: communications (87) Probable cause: trapsWillNotBeSent (822)	Severity: Major Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): No	This user-defined alarm is raised when the NE is unable to send trapsbecause the NE configuration is one of thefollowing:- The Management IP Selection is set to Out Of Band Only, thePrimaryRoute Preference is set to In Band, and the SecondaryRoute Preference is set to None.- The Management IP Selection is set to In Band Only, the PrimaryRoute Preference is set to Out Of Band, and theSecondary Route Preference is set to None.
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications (87) Probable cause: trapsRedundancyMissing (823)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): Yes	The user-defined alarm is raised when NE management redundancy isconfigured without trap route preferenceredundancy.
Name: UnidentifiedNode (1922) Type: communicationsAlarm (4) Probable cause: unidentifiedNode (922)	Severity: Major Object Type (class): DiscoveredNode Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when the node being discovered can not be properly identified.
Name: UnmanageFailed (300) Type: discoveryControlAlarm (33) Probable cause: unableToDeleteNode (231)	Severity: Warning Object Type (class): NodeDiscoveryControl Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when an attempt to unmanage an NE fails.
Name: UnsupportedNode (288) Type: configurationAlarm (11) Probable cause: unsupportedNode (219)	Severity: Warning Object Type (class): Topology Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when, during network discovery, the 5620 SAM detects an NE that uses an unsupported device software version. The alarm information includes the discovery rule ID and the IP address of the NE.

(11 of 12)

Alarm	Attributes	Description
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm (11) Probable cause: upgradedImageNotBooted (137)	Severity: Warning Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when the software version that an NE reportsaftera software upgrade does not match the version of thesoftware used for the upgrade.
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm (3) Probable cause: wrongCpaaSoftwareVersion (559)	Severity: Critical Object Type (class): NetworkElement Domain: netw Implicitly cleared (self-clearing): Yes	The alarm is raised when the 7701 CPAA softwareis the wrong versionand requires an upgrade.
Name: YellowAlarmThresholdReached (245) Type: communicationsAlarm (4) Probable cause: tooManyAlarms (182)	Severity: Critical Object Type (class): NmsSystem Domain: netw Implicitly cleared (self-clearing): No	The alarm is raised when the number of outstanding 5620 SAM alarms reaches the yellow threshold. When this happens, the 5620 SAM discards non-critical alarms to keep the number below the threshold.

(12 of 12)

Table 3-47 Domain: optical

Alarm	Attributes	Description
Name: SystemModeChange (1923) Type: equipmentAlarm (3) Probable cause: systemModeChange (923)	Severity: Major Object Type (class): OpticalNeProperties Domain: optical Implicitly cleared (self-clearing): No	The alarm is raised when an NE undergoes a system mode change, for ex. from SONET to SDH mode. The alarm information includes the Site ID, old system mode value and new system mode value.

Table 3-48 Domain: ospf

Alarm	Attributes	Description
Name: AreaTypeMismatch (38) Type: configurationAlarm (11) Probable cause: areaTypeMisconfigured (34)	Severity: Warning Object Type (class): Area Domain: ospf Implicitly cleared (self-clearing): Yes	The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.
Name: InterfaceDbDescriptAuthFailure (46) Type: authenticationAlarm (14) Probable causes: • authTypeMismatch (45) • authFailure (46)	Severity: Warning Object Type (class): Interface Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a dbDescript packet on a non-virtual interface from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.

(1 of 12)

Alarm	Attributes	Description
Name: InterfaceDbDescriptConfig (40) Type: configurationAlarm (11) Probable causes: • badVersion (35) • areaMismatch (36) • unknownNbmaNbr (37) • unknownVirtualNbr (38) • netMaskMismatch (39) • helloIntervalMismatch (40) • deadIntervalMismatch (41) • optionMismatch (42) • mtuMismatch (43) • noError (44) • duplicateRouterId (168) • ifTypeMismatch (187) • nullRouterId (188) • ifAdminDown (834) • ifPassive (835)	Severity: Warning Object Type (class): Interface Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a dbDescript packet on a non-virtual interface from an NE whose configuration parameters conflict with the local NE configuration parameters.
Name: InterfaceHelloAuthFailure (45) Type: authenticationAlarm (14) Probable causes: • authTypeMismatch (45) • authFailure (46)	Severity: Warning Object Type (class): Interface Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a hello packet on a non-virtual interface from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.
Name: InterfaceHelloConfig (39) Type: configurationAlarm (11) Probable causes: • badVersion (35) • areaMismatch (36) • unknownNbmaNbr (37) • unknownVirtualNbr (38) • netMaskMismatch (39) • helloIntervalMismatch (40) • deadIntervalMismatch (41) • optionMismatch (42) • mtuMismatch (43) • noError (44) • duplicateRouterId (168) • ifTypeMismatch (187) • nullRouterId (188) • ifAdminDown (834) • ifPassive (835)	Severity: Warning Object Type (class): Interface Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a hello packet on a non-virtual interface from an NE whose configuration parameters conflict with the local NE configuration parameters.
Name: InterfaceLsAckAuthFailure (49) Type: authenticationAlarm (14) Probable causes: • authTypeMismatch (45) • authFailure (46)	Severity: Warning Object Type (class): Interface Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives an lsAck packet on a non-virtual interface from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.

(2 of 12)

Alarm	Attributes	Description
Name: InterfaceLsAckConfig (43) Type: configurationAlarm (11) Probable causes: • badVersion (35) • areaMismatch (36) • unknownNbmaNbr (37) • unknownVirtualNbr (38) • netMaskMismatch (39) • helloIntervalMismatch (40) • deadIntervalMismatch (41) • optionMismatch (42) • mtuMismatch (43) • noError (44) • duplicateRouterId (168) • ifTypeMismatch (187) • nullRouterId (188) • ifAdminDown (834) • ifPassive (835)	Severity: Warning Object Type (class): Interface Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives an lsAck packet on a non-virtual interface from an NE whose configuration parameters conflict with the local NE configuration parameters.
Name: InterfaceLsReqAuthFailure (47) Type: authenticationAlarm (14) Probable causes: • authTypeMismatch (45) • authFailure (46)	Severity: Warning Object Type (class): Interface Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives an lsReq packet on a non-virtual interface from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.
Name: InterfaceLsReqConfig (41) Type: configurationAlarm (11) Probable causes: • badVersion (35) • areaMismatch (36) • unknownNbmaNbr (37) • unknownVirtualNbr (38) • netMaskMismatch (39) • helloIntervalMismatch (40) • deadIntervalMismatch (41) • optionMismatch (42) • mtuMismatch (43) • noError (44) • duplicateRouterId (168) • ifTypeMismatch (187) • nullRouterId (188) • ifAdminDown (834) • ifPassive (835)	Severity: Warning Object Type (class): Interface Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives an lsReq packet on a non-virtual interface from an NE whose configuration parameters conflict with the local NE configuration parameters.
Name: InterfaceLsUpdateAuthFailure (48) Type: authenticationAlarm (14) Probable causes: • authTypeMismatch (45) • authFailure (46)	Severity: Warning Object Type (class): Interface Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives an lsUpdate packet on a non-virtual interface from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.

(3 of 12)

Alarm	Attributes	Description
Name: InterfaceLsUpdateConfig (42) Type: configurationAlarm (11) Probable causes: • badVersion (35) • areaMismatch (36) • unknownNbmaNbr (37) • unknownVirtualNbr (38) • netMaskMismatch (39) • helloIntervalMismatch (40) • deadIntervalMismatch (41) • optionMismatch (42) • mtuMismatch (43) • noError (44) • duplicateRouterId (168) • ifTypeMismatch (187) • nullRouterId (188) • ifAdminDown (834) • ifPassive (835)	Severity: Warning Object Type (class): Interface Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives an lsUpdate packet on a non-virtual interface from an NE whose configuration parameters conflict with the local NE configuration parameters.
Name: InterfaceNeighborDown (661) Type: NeighborDown (20) Probable cause: NeighborDown (103)	Severity: Warning Object Type (class): Interface Domain: ospf Implicitly cleared (self-clearing): Yes	The alarm is raised when an interface neighbor is operationally down.
Name: InterfaceNullPacketAuthFailure (50) Type: authenticationAlarm (14) Probable causes: • authTypeMismatch (45) • authFailure (46)	Severity: Warning Object Type (class): Interface Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a null packet on a non-virtual interface from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.
Name: InterfaceNullPacketConfig (44) Type: configurationAlarm (11) Probable causes: • badVersion (35) • areaMismatch (36) • unknownNbmaNbr (37) • unknownVirtualNbr (38) • netMaskMismatch (39) • helloIntervalMismatch (40) • deadIntervalMismatch (41) • optionMismatch (42) • mtuMismatch (43) • noError (44) • duplicateRouterId (168) • ifTypeMismatch (187) • nullRouterId (188) • ifAdminDown (834) • ifPassive (835)	Severity: Warning Object Type (class): Interface Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a null packet on a non-virtual interface from an NE whose configuration parameters conflict with the local NE configuration parameters.

(4 of 12)

Alarm	Attributes	Description
Name: InterfaceRxBadPacket (51) Type: communicationsAlarm (4) Probable causes: • hello (47) • dbDescript (48) • lsReq (49) • lsUpdate (50) • lsAck (51) • nullPacket (52)	Severity: Warning Object Type (class): Interface Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE cannot parse an OSPF packet that it receives on a non-virtual interface.
Name: LsdbOverflow (53) Type: equipmentAlarm (3) Probable cause: resourceFull (53)	Severity: Major Object Type (class): Site Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when the number of received external LSAs exceeds the configured number allowed. By default, there is no limit. The alarm information includes the configured LSDB limit and one of the following LSDB overflow states:- 0, which means no overflow- 1, which means nearing limit- 2, which means limit exceeded
Name: NeighborDown (121) Type: NeighborDown (20) Probable cause: NeighborDown (103)	Severity: Major Object Type (class): AbstractNeighbor Domain: ospf Implicitly cleared (self-clearing): Yes	The alarm is raised when an OSPF interface neighbor is operationally Down.
Name: OspfExportLimitDropped (1924) Type: configurationAlarm (11) Probable cause: exportLimitDropped (598)	Severity: Warning Object Type (class): Site Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when the total number of exported routes from the route table tothis OSPF level drops below the configured export limit
Name: OspfExportLimitReached (1925) Type: configurationAlarm (11) Probable cause: exportLimitReached (599)	Severity: Warning Object Type (class): Site Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when the total number of routes for the level is equal to the configuredlimit for exported routes
Name: OspfExportLimitWarning (1926) Type: configurationAlarm (11) Probable cause: exportLimitWarning (600)	Severity: Warning Object Type (class): Site Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when the total number of exported routes or the level is equal tothe configured percent, vRtrIsisExportLimitLogPercent of the export limit
Name: OspfIfTxRetransmit (662) Type: communicationsAlarm (4) Probable causes: • hello (47) • dbDescript (48) • lsReq (49) • lsUpdate (50) • lsAck (51) • nullPacket (52)	Severity: Warning Object Type (class): Interface Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE retransmits an OSPF packet. The alarm information includes the NE ID of the OSPF neighbor.The alarm is not raised against a Release 4.0 or later NE.
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown (24) Probable cause: OspfInterfaceDown (112)	Severity: Warning Object Type (class): Interface Domain: ospf Implicitly cleared (self-clearing): Yes	The alarm is raised when an OSPF interface is operationally down.

(5 of 12)

Alarm	Attributes	Description
Name: ShamLinkDbDescriptAuthFailure (663) Type: authenticationAlarm (14) Probable causes: • authTypeMismatch (45) • authFailure (46)	Severity: Warning Object Type (class): ShamLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a dbDescript packet on a sham link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.
Name: ShamLinkDbDescriptConfig (664) Type: configurationAlarm (11) Probable causes: • badVersion (35) • areaMismatch (36) • unknownNbmaNbr (37) • unknownVirtualNbr (38) • netMaskMismatch (39) • helloIntervalMismatch (40) • deadIntervalMismatch (41) • optionMismatch (42) • mtuMismatch (43) • noError (44) • duplicateRouterId (168) • ifAdminDown (834) • ifPassive (835)	Severity: Warning Object Type (class): ShamLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a dbDescript packet on a sham link from an NE whose configuration parameters conflict with the local NE configuration parameters.
Name: ShamLinkDown (665) Type: ShamLinkAlarm (57) Probable cause: ShamLinkDown (492)	Severity: Critical Object Type (class): ShamLink Domain: ospf Implicitly cleared (self-clearing): Yes	The alarm is raised when a sham link is operationally down.
Name: ShamLinkHelloAuthFailure (666) Type: authenticationAlarm (14) Probable causes: • authTypeMismatch (45) • authFailure (46)	Severity: Warning Object Type (class): ShamLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a hello packet on a sham link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.
Name: ShamLinkHelloConfig (667) Type: configurationAlarm (11) Probable causes: • badVersion (35) • areaMismatch (36) • unknownNbmaNbr (37) • unknownVirtualNbr (38) • netMaskMismatch (39) • helloIntervalMismatch (40) • deadIntervalMismatch (41) • optionMismatch (42) • mtuMismatch (43) • noError (44) • duplicateRouterId (168) • ifAdminDown (834) • ifPassive (835)	Severity: Warning Object Type (class): ShamLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a hello packet on a sham link from an NE whose configuration parameters conflict with the local NE configuration parameters.

(6 of 12)

Alarm	Attributes	Description
Name: ShamLinkLsAckAuthFailure (668) Type: authenticationAlarm (14) Probable causes: • authTypeMismatch (45) • authFailure (46)	Severity: Warning Object Type (class): ShamLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives an lsAck packet on a sham link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.
Name: ShamLinkLsAckConfig (669) Type: configurationAlarm (11) Probable causes: • badVersion (35) • areaMismatch (36) • unknownNbmaNbr (37) • unknownVirtualNbr (38) • netMaskMismatch (39) • helloIntervalMismatch (40) • deadIntervalMismatch (41) • optionMismatch (42) • mtuMismatch (43) • noError (44) • duplicateRouterId (168) • ifAdminDown (834) • ifPassive (835)	Severity: Warning Object Type (class): ShamLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives an lsAck packet on a sham link from an NE whose configuration parameters conflict with the local NE configuration parameters.
Name: ShamLinkLsReqAuthFailure (670) Type: authenticationAlarm (14) Probable causes: • authTypeMismatch (45) • authFailure (46)	Severity: Warning Object Type (class): ShamLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives an lsReq packet on a sham link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.
Name: ShamLinkLsReqConfig (671) Type: configurationAlarm (11) Probable causes: • badVersion (35) • areaMismatch (36) • unknownNbmaNbr (37) • unknownVirtualNbr (38) • netMaskMismatch (39) • helloIntervalMismatch (40) • deadIntervalMismatch (41) • optionMismatch (42) • mtuMismatch (43) • noError (44) • duplicateRouterId (168) • ifAdminDown (834) • ifPassive (835)	Severity: Warning Object Type (class): ShamLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives an lsReq packet on a sham link from an NE whose configuration parameters conflict with the local NE configuration parameters.
Name: ShamLinkLsUpdateAuthFailure (672) Type: authenticationAlarm (14) Probable causes: • authTypeMismatch (45) • authFailure (46)	Severity: Warning Object Type (class): ShamLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives an lsUpdate packet on a sham link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.

(7 of 12)

Alarm	Attributes	Description
Name: ShamLinkLsUpdateConfig (673) Type: configurationAlarm (11) Probable causes: • badVersion (35) • areaMismatch (36) • unknownNbmaNbr (37) • unknownVirtualNbr (38) • netMaskMismatch (39) • helloIntervalMismatch (40) • deadIntervalMismatch (41) • optionMismatch (42) • mtuMismatch (43) • noError (44) • duplicateRouterId (168) • ifAdminDown (834) • ifPassive (835)	Severity: Warning Object Type (class): ShamLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives an lsUpdate packet on a sham link from an NE whose configuration parameters conflict with the local NE configuration parameters.
Name: ShamLinkNullPacketAuthFailure (674) Type: authenticationAlarm (14) Probable causes: • authTypeMismatch (45) • authFailure (46)	Severity: Warning Object Type (class): ShamLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a null packet on a sham link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.
Name: ShamLinkNullPacketConfig (675) Type: configurationAlarm (11) Probable causes: • badVersion (35) • areaMismatch (36) • unknownNbmaNbr (37) • unknownVirtualNbr (38) • netMaskMismatch (39) • helloIntervalMismatch (40) • deadIntervalMismatch (41) • optionMismatch (42) • mtuMismatch (43) • noError (44) • duplicateRouterId (168) • ifAdminDown (834) • ifPassive (835)	Severity: Warning Object Type (class): ShamLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a null packet on a sham link from an NE whose configuration parameters conflict with the local NE configuration parameters.
Name: ShamLinkRxBadPacket (676) Type: communicationsAlarm (4) Probable causes: • hello (47) • dbDescript (48) • lsReq (49) • lsUpdate (50) • lsAck (51) • nullPacket (52)	Severity: Warning Object Type (class): ShamLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE cannot parse an OSPF packet that it receives on a sham link.

(8 of 12)

Alarm	Attributes	Description
Name: TxRetransmit (266) Type: communicationsAlarm (4) Probable causes: • hello (47) • dbDescript (48) • lsReq (49) • lsUpdate (50) • lsAck (51) • nullPacket (52)	Severity: Warning Object Type (class): ShamLink, VirtualLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE retransmits an OSPF packet on a non-virtual interface. The alarm information includes the NE ID of the OSPF neighbor.
Name: VirtualLinkDbDescriptAuthFailure (61) Type: authenticationAlarm (14) Probable causes: • authTypeMismatch (45) • authFailure (46)	Severity: Warning Object Type (class): VirtualLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a dbDescript packet on a virtual link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.
Name: VirtualLinkDbDescriptConfig (55) Type: configurationAlarm (11) Probable causes: • badVersion (35) • areaMismatch (36) • unknownNbmaNbr (37) • unknownVirtualNbr (38) • netMaskMismatch (39) • helloIntervalMismatch (40) • deadIntervalMismatch (41) • optionMismatch (42) • mtuMismatch (43) • noError (44) • duplicateRouterId (168) • ifAdminDown (834) • ifPassive (835)	Severity: Warning Object Type (class): VirtualLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a dbDescript packet on a virtual link from an NE whose configuration parameters conflict with the local NE configuration parameters.
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm (21) Probable cause: VirtualLinkDown (104)	Severity: Warning Object Type (class): VirtualLink Domain: ospf Implicitly cleared (self-clearing): Yes	The alarm is raised when a virtual link is Down.
Name: VirtualLinkHelloAuthFailure (60) Type: authenticationAlarm (14) Probable causes: • authTypeMismatch (45) • authFailure (46)	Severity: Warning Object Type (class): VirtualLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a hello packet on a virtual link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.

(9 of 12)

Alarm	Attributes	Description
Name: VirtualLinkHelloConfig (54) Type: configurationAlarm (11) Probable causes: • badVersion (35) • areaMismatch (36) • unknownNbmaNbr (37) • unknownVirtualNbr (38) • netMaskMismatch (39) • helloIntervalMismatch (40) • deadIntervalMismatch (41) • optionMismatch (42) • mtuMismatch (43) • noError (44) • duplicateRouterId (168) • ifAdminDown (834) • ifPassive (835)	Severity: Warning Object Type (class): VirtualLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a hello packet on a virtual link from an NE whose configuration parameters conflict with the local NE configuration parameters.
Name: VirtualLinkLsAckAuthFailure (64) Type: authenticationAlarm (14) Probable causes: • authTypeMismatch (45) • authFailure (46)	Severity: Warning Object Type (class): VirtualLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives an lsAck packet on a virtual link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.
Name: VirtualLinkLsAckConfig (58) Type: configurationAlarm (11) Probable causes: • badVersion (35) • areaMismatch (36) • unknownNbmaNbr (37) • unknownVirtualNbr (38) • netMaskMismatch (39) • helloIntervalMismatch (40) • deadIntervalMismatch (41) • optionMismatch (42) • mtuMismatch (43) • noError (44) • duplicateRouterId (168) • ifAdminDown (834) • ifPassive (835)	Severity: Warning Object Type (class): VirtualLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives an lsAck packet on a virtual link from an NE whose configuration parameters conflict with the local NE configuration parameters.
Name: VirtualLinkLsReqAuthFailure (62) Type: authenticationAlarm (14) Probable causes: • authTypeMismatch (45) • authFailure (46)	Severity: Warning Object Type (class): VirtualLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives an lsReq packet on a virtual link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.

(10 of 12)

Alarm	Attributes	Description
Name: VirtualLinkLsReqConfig (56) Type: configurationAlarm (11) Probable causes: • badVersion (35) • areaMismatch (36) • unknownNbmaNbr (37) • unknownVirtualNbr (38) • netMaskMismatch (39) • helloIntervalMismatch (40) • deadIntervalMismatch (41) • optionMismatch (42) • mtuMismatch (43) • noError (44) • duplicateRouterId (168) • ifAdminDown (834) • ifPassive (835)	Severity: Warning Object Type (class): VirtualLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives an lsReq packet on a virtual link from an NE whose configuration parameters conflict with the local NE configuration parameters.
Name: VirtualLinkLsUpdateAuthFailure (63) Type: authenticationAlarm (14) Probable causes: • authTypeMismatch (45) • authFailure (46)	Severity: Warning Object Type (class): VirtualLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives an lsReq packet on a virtual link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.
Name: VirtualLinkLsUpdateConfig (57) Type: configurationAlarm (11) Probable causes: • badVersion (35) • areaMismatch (36) • unknownNbmaNbr (37) • unknownVirtualNbr (38) • netMaskMismatch (39) • helloIntervalMismatch (40) • deadIntervalMismatch (41) • optionMismatch (42) • mtuMismatch (43) • noError (44) • duplicateRouterId (168) • ifAdminDown (834) • ifPassive (835)	Severity: Warning Object Type (class): VirtualLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives an lsUpdate packet on a virtual link from an NE whose configuration parameters conflict with the local NE configuration parameters.
Name: VirtualLinkNullPacketAuthFailure (65) Type: authenticationAlarm (14) Probable causes: • authTypeMismatch (45) • authFailure (46)	Severity: Warning Object Type (class): VirtualLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a null packet on a virtual link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.

(11 of 12)

Alarm	Attributes	Description
Name: VirtualLinkNullPacketConfig (59) Type: configurationAlarm (11) Probable causes: • badVersion (35) • areaMismatch (36) • unknownNbmaNbr (37) • unknownVirtualNbr (38) • netMaskMismatch (39) • helloIntervalMismatch (40) • deadIntervalMismatch (41) • optionMismatch (42) • mtuMismatch (43) • noError (44) • duplicateRouterId (168) • ifAdminDown (834) • ifPassive (835)	Severity: Warning Object Type (class): VirtualLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a null packet on a virtual link from an NE whose configuration parameters conflict with the local NE configuration parameters.
Name: VirtualLinkRxBadPacket (66) Type: communicationsAlarm (4) Probable causes: • hello (47) • dbDescript (48) • lsReq (49) • lsUpdate (50) • lsAck (51) • nullPacket (52)	Severity: Warning Object Type (class): VirtualLink Domain: ospf Implicitly cleared (self-clearing): No	The alarm is raised when an NE cannot parse an OSPF packet that it receives on a virtual interface.
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown (22) Probable cause: VirtualNeighborDown (105)	Severity: Warning Object Type (class): ShamLink, VirtualLink Domain: ospf Implicitly cleared (self-clearing): Yes	The alarm is raised when a neighbor virtual link is operationally down.

(12 of 12)

Table 3-49 Domain: pim

Alarm	Attributes	Description
Name: DataMtReused (361) Type: dataMtReusedAlarm (37) Probable cause: DataMtReused (258)	Severity: Warning Object Type (class): DataMtInterface Domain: pim Implicitly cleared (self-clearing): No	The alarm is raised when a data MDT is reused.
Name: GroupInSSMRange (187) Type: configurationAlarm (11) Probable cause: STARGGroupInSSMRange (147)	Severity: Warning Object Type (class): Site Domain: pim Implicitly cleared (self-clearing): No	The alarm is raised when an NE receives a PIM register, PIM (*,G) assert, PIM (*,G) join/prune, or an IGMP local membership message for a group defined in the SSM address range.
Name: InvalidJoinPrune (185) Type: communicationsAlarm (4) Probable cause: InvalidJoinPruneReceived (145)	Severity: Warning Object Type (class): Site Domain: pim Implicitly cleared (self-clearing): No	The alarm is raised when the RP address in a Join Prune message is not the RP for the group specified in the message.

(1 of 2)

Alarm	Attributes	Description
Name: InvalidRegister (186) Type: communicationsAlarm (4) Probable cause: InvalidJoinRegisterReceived (146)	Severity: Warning Object Type (class): Site Domain: pim Implicitly cleared (self-clearing): No	The alarm is raised when the RP address in a Register message is not the RP for the group specified in the message.
Name: invalidRPLoopbackInterfaceConfig (269) Type: configurationAlarm (11) Probable cause: invalidRPLoopbackIfConfig (201)	Severity: Warning Object Type (class): VirtualAnyCastRP Domain: pim Implicitly cleared (self-clearing): Yes	The alarm is raised when an RP loopback interface configuration is invalid.
Name: McacPolicyDropped (341) Type: communicationsAlarm (4) Probable cause: pimGroupOnSapDropped (266)	Severity: Major Object Type (class): Interface Domain: pim Implicitly cleared (self-clearing): No	The alarm is raised when a PIM group is dropped because a multicast CAC policy is applied.
Name: mismatchAnyCastRPTypes (270) Type: configurationAlarm (11) Probable cause: mismatchAnyCastRPTypes (202)	Severity: Warning Object Type (class): AnyCastRP Domain: pim Implicitly cleared (self-clearing): No	The alarm is raised when there is an anycast RP type mismatch.
Name: missingStaticRPConfigurations (268) Type: configurationAlarm (11) Probable cause: missingStaticRPConfigurations (200)	Severity: Warning Object Type (class): VirtualAnyCastRP Domain: pim Implicitly cleared (self-clearing): Yes	The alarm is raised when a static RP configuration is missing.
Name: NeighborLoss (188) Type: communicationsAlarm (4) Probable cause: NeighborConnectionLost (148)	Severity: Warning Object Type (class): Interface Domain: pim Implicitly cleared (self-clearing): Yes	The alarm is raised when the connection to a neighbor is lost.
Name: peerSetConfigurationIssue (267) Type: configurationAlarm (11) Probable cause: mismatchPeerSets (199)	Severity: Major Object Type (class): VirtualAnyCastRP Domain: pim Implicitly cleared (self-clearing): Yes	The alarm is raised when a peer set is misconfigured.
Name: PimDown (184) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): Site Domain: pim Implicitly cleared (self-clearing): Yes	This alarm is raised when a PIM site is administratively Up but operationally Down.The alarm clears when the site becomes operationally Up or administratively Down.

(2 of 2)

Table 3-50 Domain: policy

Alarm	Attributes	Description
Name: DefaultInstanceInconsistency (211) Type: ConfigurationAlarm (15) Probable cause: multipleDefaultInstancesEncountered (54)	Severity: Warning Object Type (class): Manager Domain: policy Implicitly cleared (self-clearing): Yes	The alarm is raised when an accounting policy is the default for more then one service type or more then one network type.

(1 of 2)

Alarm	Attributes	Description
Name: TemplateInconsistency (189) Type: ConfigurationAlarm (15) Probable cause: templatePolicyMismatch (149)	Severity: Warning Object Type (class): PolicyDefinition Domain: policy Implicitly cleared (self-clearing): Yes	The alarm is raised when there is a parameter type or value mismatch between a global policy and a local policy.

(2 of 2)

Table 3-51 Domain: ppp

Alarm	Attributes	Description
Name: PppLoopbackDetected (362) Type: configurationAlarm (11) Probable cause: PppLoopbackDetected (259)	Severity: Major Object Type (class): Interface Domain: ppp Implicitly cleared (self-clearing): Yes	The alarm is raised when the value of tmnxPppLocalMagicNumber is the same as the value of tmnxPppRemoteMagicNumber, which indicates that the link may be looped back.

Table 3-52 Domain: radioequipment

Alarm	Attributes	Description
Name: AtpcLoopProblem (1142) Type: communicationsAlarm (4) Probable cause: atpcLoopProblem (848)	Severity: Minor Object Type (class): RadioPortSpecifics Domain: radioequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a receiver protection switchover fails.
Name: BandwidthOverFlow (1143) Type: communicationsAlarm (4) Probable cause: bandwidthOverFlow (849)	Severity: Major Object Type (class): RadioPortSpecifics Domain: radioequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a receiver protection switchover fails.
Name: CableLOS (678) Type: communicationsAlarm (4) Probable cause: cableLOS (493)	Severity: Major Object Type (class): RadioPortSpecifics Domain: radioequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an MSS detects a cable LOS event.
Name: CrossConnectionFail (679) Type: communicationsAlarm (4) Probable cause: crossConnectionFail (494)	Severity: Major Object Type (class): RadioPortSpecifics Domain: radioequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an MSS TDM cross-connection fails.
Name: DemFail (680) Type: communicationsAlarm (4) Probable cause: demFail (495)	Severity: Major Object Type (class): RadioPortSpecifics Domain: radioequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an MSS demodulation function fails.

(1 of 3)

Alarm	Attributes	Description
Name: EarlyWarning (681) Type: communicationsAlarm (4) Probable cause: earlyWarning (496)	Severity: Warning Object Type (class): RadioPortSpecifics Domain: radioequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an MSS detects an early warning event.
Name: HighBER (682) Type: communicationsAlarm (4) Probable cause: highBER (497)	Severity: Minor Object Type (class): RadioPortSpecifics Domain: radioequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an MSS detects a high BER.
Name: IncompatibleFrequency (683) Type: communicationsAlarm (4) Probable cause: incompatibleFrequency (498)	Severity: Major Object Type (class): RadioPortSpecifics Domain: radioequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a provisioned MSS frequency is incompatible with the MSS hardware.
Name: IncompatibleModulationParam (1144) Type: communicationsAlarm (4) Probable cause: incompatibleModulation (850)	Severity: Minor Object Type (class): RadioPortSpecifics Domain: radioequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a receiver protection switchover fails.
Name: IncompatiblePTX (684) Type: communicationsAlarm (4) Probable cause: incompatiblePTX (499)	Severity: Major Object Type (class): RadioPortSpecifics Domain: radioequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the provisioned MSS transmit power is incompatible with the MSS hardware.
Name: IncompatibleShifter (685) Type: communicationsAlarm (4) Probable cause: incompatibleShifter (500)	Severity: Major Object Type (class): RadioPortSpecifics Domain: radioequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when the provisioned MSS shifter parameters are incompatible with the MSS hardware.
Name: LinkIdentifierMismatch (686) Type: communicationsAlarm (4) Probable cause: linkIdentifierMismatch (501)	Severity: Major Object Type (class): RadioPortSpecifics Domain: radioequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an MSS detects a link identifier mismatch.
Name: LoopProblem (1145) Type: communicationsAlarm (4) Probable cause: loopProblem (851)	Severity: Minor Object Type (class): RadioPortSpecifics Domain: radioequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a receiver protection switchover fails.
Name: RPSFail (1085) Type: communicationsAlarm (4) Probable cause: receiverProtectionFail (824)	Severity: Minor Object Type (class): RadioPortSpecifics Domain: radioequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a receiver protection switchover fails.

(2 of 3)

Alarm	Attributes	Description
Name: RxFail (687) Type: communicationsAlarm (4) Probable cause: rxFail (502)	Severity: Major Object Type (class): RadioPortSpecifics Domain: radioequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an MSS detects a receive failure.

(3 of 3)

Table 3-53 Domain: radiusaccounting

Alarm	Attributes	Description
Name: RadisuAcctPlcyFailure (363) Type: radiusAccountingPolicyAlarm (38) Probable cause: radiusAccountingRequestFailure (260)	Severity: Major Object Type (class): Policy Domain: radiusaccounting Implicitly cleared (self-clearing): No	The alarm is raised when a RADIUS accounting request is not successfully sent to any of theRADIUS servers specified in the RADIUS accounting policy.

Table 3-54 Domain: resiliency

Alarm	Attributes	Description
Name: ResiliencySapDeleted (688) Type: resiliencyAlarm (58) Probable cause: resiliencySapDeleted (503)	Severity: Major Object Type (class): HsdpaResiliency Domain: resiliency Implicitly cleared (self-clearing): Yes	The alarm is raised when a SAP that is used for resiliency is deleted.
Name: ResiliencyServiceSwitch (689) Type: resiliencyAlarm (58) Probable cause: secondaryServiceSiteActive (504)	Severity: Major Object Type (class): HsdpaResiliency Domain: resiliency Implicitly cleared (self-clearing): Yes	The alarm is raised when a secondary service becomes active.
Name: ResiliencySiteDeleted (690) Type: resiliencyAlarm (58) Probable cause: secondaryServiceSiteDeleted (505)	Severity: Major Object Type (class): HsdpaResiliency Domain: resiliency Implicitly cleared (self-clearing): Yes	The alarm is raised when a secondary service site is deleted.

Table 3-55 Domain: ressubscr

Alarm	Attributes	Description
Name: HostConnectivityLostRateExceeded (276) Type: communicationsAlarm (4) Probable causes: • hostDown (208) • trapDropped (209)	Severity: Major Object Type (class): ShcvSite Domain: ressubscr Implicitly cleared (self-clearing): No	The alarm is raised when the trapDroppedRaisesAlarm parameter is enabled and the maximum allowed number of SHCV host connectivity loss events on a SAP is exceeded. The SHCV action in response to the alarm is specified by the maxHostLostConnectivityRate parameter. If the specified action is to remove the host information, the host information is removed and the connectivity of the host is not subsequently verified.
Name: NatL2AwSubIcmpPortUsageHigh (1086) Type: equipmentAlarm (3) Probable cause: resourceFull (53)	Severity: Major Object Type (class): ResidentialSubscriberInstance Domain: ressubscr Implicitly cleared (self-clearing): Yes	The alarm is raised when the ICMP port usage of an L2-aware NAT subscriber reaches the high or low watermark.
Name: NatL2AwSubSessionUsageHigh (1087) Type: equipmentAlarm (3) Probable cause: resourceFull (53)	Severity: Major Object Type (class): ResidentialSubscriberInstance Domain: ressubscr Implicitly cleared (self-clearing): Yes	The alarm is raised when the session usage of an L2-aware NAT subscriber reaches the high or low watermark.
Name: NatL2AwSubTcpPortUsageHigh (1088) Type: equipmentAlarm (3) Probable cause: resourceFull (53)	Severity: Major Object Type (class): ResidentialSubscriberInstance Domain: ressubscr Implicitly cleared (self-clearing): Yes	The alarm is raised when the TCP port usage of an L2-aware NAT subscriber reaches the high or low watermark.
Name: NatL2AwSubUdpPortUsageHigh (1089) Type: equipmentAlarm (3) Probable cause: resourceFull (53)	Severity: Major Object Type (class): ResidentialSubscriberInstance Domain: ressubscr Implicitly cleared (self-clearing): Yes	The alarm is raised when the UDP port usage of an L2-aware NAT subscriber reaches the high or low watermark.

Table 3-56 Domain: rip

Alarm	Attributes	Description
Name: GroupDown (69) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): Group Domain: rip Implicitly cleared (self-clearing): Yes	The alarm is raised when a RIP group has an Operational State other than Up, and the Administrative State is Up.
Name: RipAuthenticationFailure (70) Type: authenticationAlarm (14) Probable cause: authFailure (46)	Severity: Warning Object Type (class): Interface Domain: rip Implicitly cleared (self-clearing): No	The alarm is raised when a peer authentication failure occurs. The alarm information includes the peer address.

(1 of 2)

Alarm	Attributes	Description
Name: RipAuthenticationMismatch (71) Type: authenticationAlarm (14) Probable cause: authTypeMismatch (45)	Severity: Warning Object Type (class): Interface Domain: rip Implicitly cleared (self-clearing): No	The alarm is raised when a peer authentication mismatch occurs. The alarm indicates the peer address.
Name: RipDown (72) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): Site Domain: rip Implicitly cleared (self-clearing): Yes	The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.
Name: RipExportLimitDropped (1927) Type: configurationAlarm (11) Probable cause: exportLimitDropped (598)	Severity: Warning Object Type (class): Site Domain: rip Implicitly cleared (self-clearing): No	The alarm is raised when the total number of exported routes from the route table tothis RIP level drops below the configured export limit
Name: RipExportLimitReached (1928) Type: configurationAlarm (11) Probable cause: exportLimitReached (599)	Severity: Warning Object Type (class): Site Domain: rip Implicitly cleared (self-clearing): No	The alarm is raised when the total number of routes for the level is equal to the configuredlimit for exported routes
Name: RipExportLimitWarning (1929) Type: configurationAlarm (11) Probable cause: exportLimitWarning (600)	Severity: Warning Object Type (class): Site Domain: rip Implicitly cleared (self-clearing): No	The alarm is raised when the total number of exported routes or the level is equal tothe configured percent, vRtrIsisExportLimitLogPercent of the export limit
Name: ripRouteMaxLimitReached (1090) Type: ProtocolAlarm (1) Probable cause: maxRouteReached (825)	Severity: Warning Object Type (class): Site Domain: rip Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of RIP routes learned by an NE exceeds the maximum specified in the RIP configuration of the NE.

(2 of 2)

Table 3-57 Domain: rmon

Alarm	Attributes	Description
Name: IncompleteConfig (294) Type: configurationAlarm (11) Probable cause: incompleteConfig (225)	Severity: Major Object Type (class): Alarm, Event Domain: rmon Implicitly cleared (self-clearing): Yes	The alarm is raised when an object is created with default values but not yet made active.
Name: MissingFallingEvent (414) Type: configurationAlarm (11) Probable cause: incompleteConfig (225)	Severity: Major Object Type (class): Alarm Domain: rmon Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM cannot find the falling event object that is named in anRMON policy alarm definition.
Name: MissingRisingEvent (413) Type: configurationAlarm (11) Probable cause: incompleteConfig (225)	Severity: Major Object Type (class): Alarm Domain: rmon Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM cannot find the rising event object that is named in anRMON policy alarm definition.

Table 3-58 Domain: rsvp

Alarm	Attributes	Description
Name: RsvpDown (74) Type: ProtocolAlarm (1) Probable cause: protocolDown (1)	Severity: Critical Object Type (class): Site Domain: rsvp Implicitly cleared (self-clearing): Yes	The alarm is raised when an RSVP site has an Operational State other than Up, and the Administrative State is Up.
Name: SessionDown (73) Type: ProtocolAlarm (1) Probable cause: interfaceDown (32)	Severity: Critical Object Type (class): Session Domain: rsvp Implicitly cleared (self-clearing): Yes	The alarm is raised when an RSVP session is operationally down.

Table 3-59 Domain: rtr

Alarm	Attributes	Description
Name: BfdSessionDown (439) Type: bfdSessionAlarm (46) Probable cause: bfdSessionDown (346)	Severity: Warning Object Type (class): NetworkInterface Domain: rtr Implicitly cleared (self-clearing): Yes	The alarm is raised when a BFD session is operationally Down.
Name: BfdSessionMissing (438) Type: bfdSessionAlarm (46) Probable cause: bfdSessionMissing (345)	Severity: Warning Object Type (class): NetworkInterface Domain: rtr Implicitly cleared (self-clearing): Yes	The alarm is raised when a previously present BFD session is absent.
Name: CpeUnreachable (525) Type: communicationsAlarm (4) Probable cause: CpeUnreachable (334)	Severity: Major Object Type (class): StaticRoute Domain: rtr Implicitly cleared (self-clearing): Yes	The alarm is raised when the CPE associated with a static route is unreachable.
Name: SubscrAuthPolicyMisconfigured (271) Type: ConfigurationAlarm (15) Probable cause: SubscrAuthPolicyNotFound (203)	Severity: Warning Object Type (class): VirtualInterfaceConfiguration Domain: rtr Implicitly cleared (self-clearing): Yes	The alarm is raised when a subscriber authentication policy for DHCP relay is misconfigured.
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm (18) Probable cause: networkDegradation (204)	Severity: Major Object Type (class): VirtualRouter Domain: rtr Implicitly cleared (self-clearing): Yes	The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.

Table 3-60 Domain: rules

Alarm	Attributes	Description
Name: RuleRegistrationError (364) Type: ConfigurationAlarm (15) Probable cause: ruleContentsError (261)	Severity: Warning Object Type (class): RuleSet Domain: rules Implicitly cleared (self-clearing): Yes	The alarm is raised when one or more internal 5620 SAM server rule-engine rules fails to compile. The cause is typically a rule syntax error or a system error.

Table 3-61 Domain: sas

Alarm	Attributes	Description
Name: SasAccountingAlarm (691) Type: oamAlarm (18) Probable cause: noAccountingPolicy (506)	Severity: Minor Object Type (class): TestSuite Domain: sas Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM cannot find an SAA Accounting Policy.
Name: SasSlaAlarm (568) Type: oamAlarm (18) Probable cause: networkDegradation (204)	Severity: Minor Object Type (class): TestSuite Domain: sas Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects a lightweight test execution failure.
Name: SasThresholdExceededAlarm (272) Type: oamAlarm (18) Probable cause: networkDegradation (204)	Severity: Major Object Type (class): Test Domain: sas Implicitly cleared (self-clearing): Yes	The alarm is raised when a rising or falling threshold is crossed by a jitter, latency, or loss value. The alarm is raised only against a scheduled test. The alarm information includes the threshold type, the threshold setting, and the current rising or falling value.
Name: SasTooManyTestsOnNodeAlarm (287) Type: oamAlarm (18) Probable cause: tooManyTestsDeployedOnNode (220)	Severity: Major Object Type (class): NeAgent Domain: sas Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE reaches 60 percent of the allowed number of created or simultaneously executed OAM tests. An attempt to create or execute an NE schedulable test on an NE fails when the number of tests reaches 95 percent of the NE capacity. The alarm information includes the following:- the NE ID- the number of deployed tests on the NE- the allowed number of deployed tests on the NE
Name: STMSystemMultiAuxAvailable (527) Type: misConfiguration (53) Probable cause: multiAuxiliaryServersAvailable (399)	Severity: Critical Object Type (class): TestManager Domain: sas Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM detects multiple available auxiliary servers for test execution.
Name: STMSystemNotAvailable (526) Type: communicationsAlarm (4) Probable cause: noAuxiliaryServersAvailable (256)	Severity: Critical Object Type (class): TestManager Domain: sas Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM detects no available auxiliary servers for test execution.

(1 of 2)

Alarm	Attributes	Description
Name: STMTestIdRangeMismatch (792) Type: oamAlarm (18) Probable cause: testIdRangeMismatch (560)	Severity: Major Object Type (class): TestManager Domain: sas Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects an STM test ID range mismatch between the primary and standby main servers.
Name: STMTestsOutsideRange (793) Type: oamAlarm (18) Probable cause: testsOutsideRange (561)	Severity: Major Object Type (class): TestManager Domain: sas Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM detects one or more STM Tests that have IDs outside the specified range.

(2 of 2)

Table 3-62 Domain: schedule

Alarm	Attributes	Description
Name: scheduledTaskCompletionStatus (528) Type: taskCompletionAlarm (45) Probable cause: scheduledTaskCompleted (400)	Severity: Info Object Type (class): ScheduledTask Domain: schedule Implicitly cleared (self-clearing): No	The alarm is raised when the execution of a SAM scheduled task completes.

Table 3-63 Domain: security

Alarm	Attributes	Description
Name: AuthenticationFailure (128) Type: communicationsAlarm (4) Probable cause: multipleSecurityViolations (336)	Severity: Warning Object Type (class): TSecurityManager Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when a configurable number of attempts to log in to a 5620 SAM client fail. The alarm information includes the user name. The 5620 SAM deletes the alarm when the user account is deleted.
Name: AuthorizationFailure (529) Type: communicationsAlarm (4) Probable cause: multipleSecurityViolations (336)	Severity: Warning Object Type (class): TSecurityManager Domain: security Implicitly cleared (self-clearing): No	The alarm is raised when a configurable number of attempts to delete or modify an object that is not in the current user span of control fail.
Name: CpamTimedLicenseExpiryNotice (692) Type: cpamLicensingAlarm (39) Probable cause: timedcpamLicenseExpiryNotice (293)	Severity: Warning Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): No	The alarm is raised when the 5650 CPAM license timer expires. The alarm information includes the license expiry date.
Name: JMSClientMessagesRemoved (532) Type: communicationsAlarm (4) Probable cause: maximumExceededMessages (297)	Severity: Minor Object Type (class): User Domain: security Implicitly cleared (self-clearing): No	The alarm is raised when the number of JMS messages that are queued for a 5620 SAM client exceeds the allowed number. The 5620 SAM subsequently deletes messages to keep the number within the allowed range.

(1 of 5)

Alarm	Attributes	Description
Name: JMSDurableClientReset (530) Type: communicationsAlarm (4) Probable cause: jmsServerRestart (401)	Severity: Warning Object Type (class): User Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when a durable JMS client is removed from the 5620 SAM because of a JMS server restart or switchover.
Name: JMSDurableClientUnsubscribed (531) Type: communicationsAlarm (4) Probable cause: maximumExceededMessages (297)	Severity: Minor Object Type (class): User Domain: security Implicitly cleared (self-clearing): No	The alarm is raised when a durable JMS client is unsubscribed and removed from the 5620 SAM.
Name: KeyChainAuthFailure (421) Type: communicationsAlarm (4) Probable cause: keyChainAuthFailure (314)	Severity: Major Object Type (class): KeyChain Domain: security Implicitly cleared (self-clearing): No	The alarm is raised when an incoming packet is dropped because of a TCP key chain authentication failure.
Name: Licensed3RouterLimitExceeded (694) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitExceeded (285)	Severity: Critical Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of third-party routers in the 5650 CPAM network reaches 100 percent of the license capacity.
Name: Licensed3RouterLimitNearing (695) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitNearing (283)	Severity: Warning Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of third-party routers in the 5650 CPAM network reaches 75 to 90 percent of the license capacity.
Name: Licensed3RouterLimitNearlyExceeded (696) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitNearlyExceeded (284)	Severity: Major Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of third-party routers in the 5650 CPAM network reaches 90 to 100 percent of the license capacity.
Name: LicensedBigRouterLimitExceeded (709) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitExceeded (285)	Severity: Critical Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of Alcatel-Lucent large routers in the network reaches 100 percent of the 5650 CPAM license capacity.
Name: LicensedBigRouterLimitNearing (710) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitNearing (283)	Severity: Warning Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of Alcatel-Lucent large routers in the network reaches 75 to 90 percent of the 5650 CPAM license capacity.
Name: LicensedBigRouterLimitNearlyExceeded (711) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitNearlyExceeded (284)	Severity: Major Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of Alcatel-Lucent large routers in the network reaches 90 to 100 percent of the 5650 CPAM license capacity.
Name: LicensedCpaaLimitExceeded (389) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitExceeded (285)	Severity: Critical Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of 7701 CPAAs in the network reaches 100 percent of the license capacity.

(2 of 5)

Alarm	Attributes	Description
Name: LicensedCpaaLimitNearing (390) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitNearing (283)	Severity: Warning Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of 7701 CPAAs in the network reaches 75 to 90 percent of the license capacity.
Name: LicensedCpaaLimitNearlyExceeded (391) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitNearlyExceeded (284)	Severity: Major Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of 7701 CPAAs in the network reaches 90 to 100 percent of the license capacity.
Name: LicensedImpactAnalysisRouterLimitExceeded (712) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitExceeded (285)	Severity: Critical Object Type (class): CpamLicenseScenario Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of routers in a simulation scenario reaches 100 percent of the license capacity.
Name: LicensedImpactAnalysisRouterLimitNearing (713) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitNearing (283)	Severity: Warning Object Type (class): CpamLicenseScenario Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of routers in a simulation scenario reaches 75 to 90 percent of the license capacity.
Name: LicensedImpactAnalysisRouterLimitNearlyExceeded (714) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitNearlyExceeded (284)	Severity: Major Object Type (class): CpamLicenseScenario Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of routers in a simulation scenario reaches 90 to 100 percent of the license capacity.
Name: LicensedIpPathLimitExceeded (715) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitExceeded (285)	Severity: Critical Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of IP path monitors in the 5650 CPAM reaches 100 percent of the license capacity.
Name: LicensedIpPathLimitNearing (716) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitNearing (283)	Severity: Warning Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of IP path monitors in the 5650 CPAM reaches 75 to 90 percent of the license capacity.
Name: LicensedIpPathLimitNearlyExceeded (717) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitNearlyExceeded (284)	Severity: Major Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of IP path monitors in the 5650 CPAM reaches 90 to 100 percent of the license capacity.
Name: LicensedLimitExceeded (127) Type: licensingAlarm (23) Probable cause: licensedLimitExceeded (106)	Severity: Critical Object Type (class): ProductLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the license items in the network exceeds 100 percent of the licensecapacity.
Name: LicensedLimitNearing (1931) Type: licensingAlarm (23) Probable cause: licensedLimitNearing (132)	Severity: Warning Object Type (class): ProductLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the license items in the network reaches 75 to 90 percent of thelicense capacity.

(3 of 5)

Alarm	Attributes	Description
Name: LicensedLimitNearlyExceeded (1932) Type: licensingAlarm (23) Probable cause: licensedLimitNearlyExceeded (133)	Severity: Major Object Type (class): ProductLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the license items in the network reaches 90 to 100 percent of thelicense capacity.
Name: LicensedLimitReached (1933) Type: licensingAlarm (23) Probable cause: licensedLimitReached (925)	Severity: Major Object Type (class): ProductLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the license items in the network reaches 100 percent of the licensecapacity.
Name: LicensedMcRouterLimitExceeded (718) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitExceeded (285)	Severity: Critical Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of multicast routers in the 5650 CPAM reaches 100 percent of the license capacity.
Name: LicensedMcRouterLimitNearing (719) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitNearing (283)	Severity: Warning Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of multicast routers in the 5650 CPAM reaches 75 to 90 percent of the license capacity.
Name: LicensedMcRouterLimitNearlyExceeded (720) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitNearlyExceeded (284)	Severity: Major Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of multicast routers in the 5650 CPAM reaches 90 to 100 percent of the license capacity.
Name: LicensedSmallRouterLimitExceeded (727) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitExceeded (285)	Severity: Critical Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of Alcatel-Lucent small routers in the network reaches 100 percent of the 5650 CPAM license capacity.
Name: LicensedSmallRouterLimitNearing (728) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitNearing (283)	Severity: Warning Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of Alcatel-Lucent small routers in the network reaches 75 to 90 percent of the 5650 CPAM license capacity.
Name: LicensedSmallRouterLimitNearlyExceeded (729) Type: cpamLicensingAlarm (39) Probable cause: cpamLicensedLimitNearlyExceeded (284)	Severity: Major Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of Alcatel-Lucent small routers in the network reaches 90 to 100 percent of the 5650 CPAM license capacity.
Name: LicenseKeyIsInvalid (1122) Type: licensingAlarm (23) Probable cause: LicenseKeyIsInvalid (836)	Severity: Warning Object Type (class): AbstractLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM server configuration is updated with a new license key and the license key is not valid.
Name: LicenseMismatch (342) Type: licensingAlarm (23) Probable cause: licenseMismatch (247)	Severity: Critical Object Type (class): AbstractLicense Domain: security Implicitly cleared (self-clearing): No	The alarm is raised when the primary 5620 SAM main server license does not match the standby5620 SAM main server license.

(4 of 5)

Alarm	Attributes	Description
Name: LicenseMisMatch (693) Type: cpamLicensingAlarm (39) Probable cause: cpamLicenseMisMatch (507)	Severity: Critical Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): No	The alarm is raised when the primary 5650 CPAM server license does not match the standby 5650 CPAM server license.
Name: LicenseViolation (1930) Type: licensingAlarm (23) Probable cause: licenseViolation (924)	Severity: Warning Object Type (class): ProductLicense Domain: security Implicitly cleared (self-clearing): No	The alarm is raised when license violation happened.capacity.
Name: MediationAuthenticationFailure (75) Type: communicationsAlarm (4) Probable causes: • unsupportedSecLevel (55) • notInTimeWindow (56) • unknownUserName (57) • unknownEngineID (58) • wrongDigest (59) • decryptionError (60)	Severity: Warning Object Type (class): BaseMediationPolicy Domain: security Implicitly cleared (self-clearing): No	The alarm is raised when a mediation authentication failure occurs.
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm (4) Probable cause: ssh2ServerKeyMismatch (217)	Severity: Warning Object Type (class): KnownHostKey Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when a 5620 SAM main server detects a new public SSH key.
Name: RouterLimitExceedDueToMultiAdditions (602) Type: cpamLicensingAlarm (39) Probable cause: cpamRouterLimitExceedDueToMultiAdditions (448)	Severity: Critical Object Type (class): CpamLicense Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5650 CPAM cannot discover one or more routers because the license capacity is reached.
Name: TimedLicenseExpiryNotice (263) Type: licensingAlarm (23) Probable cause: timedLicenseExpiryNotice (196)	Severity: Warning Object Type (class): AbstractLicense Domain: security Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM license timer expires. The alarm information includes thelicense expiry date.
Name: UserSuspended (1123) Type: communicationsAlarm (4) Probable cause: multipleSecurityViolations (336)	Severity: Warning Object Type (class): User Domain: security Implicitly cleared (self-clearing): Yes	The alarm is raised when a user account is suspended.

(5 of 5)

Table 3-64 Domain: server

Alarm	Attributes	Description
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm (4) Probable cause: systemFailed (144)	Severity: Critical Object Type (class): AuxiliaryServer Domain: server Implicitly cleared (self-clearing): Yes	The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.

(1 of 3)

Alarm	Attributes	Description
Name: ClientDelegateServerMaxUIExceeded (730) Type: resourceAlarm (28) Probable cause: clientDelegateServerMaxUIExceeded (508)	Severity: Warning Object Type (class): ClientDelegateServer Domain: server Implicitly cleared (self-clearing): Yes	The alarm is raised when the total number of client GUI sessions on a client delegate server reaches or exceeds the configured maximum value.
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm (4) Probable cause: systemFailed (144)	Severity: Critical Object Type (class): ClientDelegateServer Domain: server Implicitly cleared (self-clearing): Yes	The alarm is raised when a client delegate server is unreachable.
Name: DiskSpaceBelowThreshold (1934) Type: serverAlarm (94) Probable cause: diskSpaceIssue (153)	Severity: Variable or indeterminate Object Type (class): SamServer Domain: server Implicitly cleared (self-clearing): No	The alarm is raised when the disk space threshold is reached.
Name: DroppedUdpPackets (1935) Type: communicationsAlarm (4) Probable cause: tooManyUdpPacketsBuffered (926)	Severity: Variable or indeterminate Object Type (class): SamServer Domain: server Implicitly cleared (self-clearing): No	The alarm is raised when the number of UDP Packets that await processing by the 5620 SAM surpasses.
Name: HostnameMismatch (732) Type: configurationAlarm (11) Probable cause: hostnameMismatch (509)	Severity: Critical Object Type (class): AuxiliaryServer Domain: server Implicitly cleared (self-clearing): No	The alarm is raised when an auxiliary server host name in a 5620 SAM main server configuration does not match the host name of the auxliary server in the local /etc/hosts file.
Name: MemoryThresholdCrossingAlarm (1936) Type: configurationAlarm (11) Probable cause: lowMemoryConfigured (927)	Severity: Variable or indeterminate Object Type (class): SamServer Domain: server Implicitly cleared (self-clearing): No	The alarm is raised when the memory of the SAM Server excceds some threshold.
Name: OneWayCommunication (733) Type: communicationsAlarm (4) Probable cause: routingConfiguration (510)	Severity: Major Object Type (class): AuxiliaryServer Domain: server Implicitly cleared (self-clearing): Yes	The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server, but the auxiliary server can communicate with the main server.
Name: PurgeFilesToFreeDiskSpace (1937) Type: serverAlarm (94) Probable cause: diskSpaceIssue (153)	Severity: Variable or indeterminate Object Type (class): SamServer Domain: server Implicitly cleared (self-clearing): No	The alarm is raised when Server deletes some files to free the disk space.
Name: RsyncDirectoryMismatch (1938) Type: serverAlarm (94) Probable cause: rsyncDirectoryMismatch (928)	Severity: Major Object Type (class): SamServer Domain: server Implicitly cleared (self-clearing): No	The alarm is raised when the rsync directories mismatch between two Servers.
Name: RsyncFilesToRemoteHost (1939) Type: communicationsAlarm (4) Probable cause: rsyncFilesIssue (929)	Severity: Variable or indeterminate Object Type (class): SamServer Domain: server Implicitly cleared (self-clearing): No	The alarm is raised when the rsync cannot sync the files with the remote server.

(2 of 3)

Alarm	Attributes	Description
Name: TimeMismatch (436) Type: configurationAlarm (11) Probable cause: timeMismatch (344)	Severity: Major Object Type (class): AuxiliaryServer Domain: server Implicitly cleared (self-clearing): No	The alarm is raised when the system time on a 5620 SAM auxiliary server station differs from the system time on a main server station.
Name: WriteFileToDisk (1940) Type: serverAlarm (94) Probable cause: diskSpaceIssue (153)	Severity: Variable or indeterminate Object Type (class): SamServer Domain: server Implicitly cleared (self-clearing): No	The alarm is raised when SAM cannot write a file to disk.

(3 of 3)

Table 3-65 Domain: service

Alarm	Attributes	Description
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm (32) Probable cause: interfaceDown (32)	Severity: Critical Object Type (class): AccessInterface Domain: service Implicitly cleared (self-clearing): Yes	The alarm is raised when an L2 or L3 interface operational state is Down and the administrative state of the associated site is Up.The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.
Name: AddressMisconfiguration (591) Type: configurationAlarm (11) Probable causes: • EpipeBackboneMacAddressMismatch (444) • BVplsSourceMacAddressDuplicate (445)	Severity: Major Object Type (class): Service Domain: service Implicitly cleared (self-clearing): Yes	The alarm is raised when B-VPLS site addresses are misconfigured. The EpipeBackboneMacAddressMismatch probable cause indicates that the backbone destination MAC address does not match the backbone source MAC address of the site on the destination NE. The BVplsSourceMacAddressDuplicate probable cause indicates that there are duplicate backbone source MAC addresses.
Name: BfdSessionDown (439) Type: bfdSessionAlarm (46) Probable cause: bfdSessionDown (346)	Severity: Warning Object Type (class): L3AccessInterface Domain: service Implicitly cleared (self-clearing): Yes	The alarm is raised when a BFD session is operationally down.
Name: BfdSessionMissing (438) Type: bfdSessionAlarm (46) Probable cause: bfdSessionMissing (345)	Severity: Warning Object Type (class): L3AccessInterface Domain: service Implicitly cleared (self-clearing): Yes	The alarm is raised when a previously present BFD session is absent.
Name: EndpointActiveObjectChanged (437) Type: redundancyAlarm (52) Probable causes: • RedundancySwitchover (317) • ForceSwitchover (318)	Severity: Warning Object Type (class): Endpoint Domain: service Implicitly cleared (self-clearing): No	The alarm is raised when an automatic or manual endpoint switchover occurs.

(1 of 3)

Alarm	Attributes	Description
Name: FrameSizeProblem (37) Type: configurationAlarm (11) Probable cause: frameSizeProblem (33)	Severity: Warning Object Type (class): Service Domain: service Implicitly cleared (self-clearing): Yes	The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.
Name: GroupInterfaceDown (441) Type: GroupInterfaceAlarm (44) Probable cause: interfaceDown (32)	Severity: Critical Object Type (class): GroupInterface Domain: service Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects that a group interface is operationally down. The alarm clears when the group interface is operationally up.
Name: InterfaceDown (36) Type: configurationAlarm (11) Probable cause: interfaceDown (32)	Severity: Major Object Type (class): RedundantInterface Domain: service Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects that a redundant interface is operationally down.
Name: SapDHCPLeaseEntriesExceeded (386) Type: communicationsAlarm (4) Probable cause: sapDHCPLeaseEntriesExceeded (290)	Severity: Major Object Type (class): AccessInterface Domain: service Implicitly cleared (self-clearing): No	The alarm is raised when the number of DHCP lease-state entries on a SAP reaches the configured maximum value. This value is defined by sapTlsDhcpLeasePopulate for a TLS VLAN service, and by vRtrIfDHCPLeasePopulate for an IES or VPRN service.
Name: sapDHCPProxyServerError (387) Type: communicationsAlarm (4) Probable cause: UnableProxyDHCPRequest (291)	Severity: Major Object Type (class): AccessInterface Domain: service Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM is unable to proxy a DHCP request.
Name: ServiceSiteDown (97) Type: serviceAlarm (16) Probable cause: siteDown (83)	Severity: Critical Object Type (class): Site Domain: service Implicitly cleared (self-clearing): Yes	The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down.
Name: SubscriberInterfaceDown (440) Type: SubscriberInterfaceAlarm (43) Probable cause: interfaceDown (32)	Severity: Critical Object Type (class): SubscriberInterface Domain: service Implicitly cleared (self-clearing): Yes	The alarm is raised when a subscriber interface is operationally down. The alarm clears when the subscriber interface is operationally up.
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm (18) Probable cause: networkDegradation (204)	Severity: Major Object Type (class): SpokeConnector Domain: service Implicitly cleared (self-clearing): Yes	The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.
Name: TestThresholdExceededAlarm2 (1918) Type: oamAlarm (18) Probable cause: networkDegradation (204)	Severity: Major Object Type (class): Site Domain: service Implicitly cleared (self-clearing): Yes	The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.
Name: TodSuiteAssignmentFailure (312) Type: todSuiteAlarm (35) Probable cause: configConflictOrResourceFull (274)	Severity: Minor Object Type (class): AccessInterface Domain: service Implicitly cleared (self-clearing): No	The alarm is raised when a Time of Day suite cannot be assigned to an aggregation scheduler, or to an L2 or L3 access interface, because of a configuration conflict or a lack of resources. The alarm is not raised against a SAP.

(2 of 3)

Alarm	Attributes	Description
Name: TopologyMisconfigured (95) Type: configurationAlarm (11) Probable cause: topologyMisconfigured (81)	Severity: Critical Object Type (class): Service Domain: service Implicitly cleared (self-clearing): Yes	The alarm is raised when the same service ID on two NEs is associated with a different service type on each NE, or when a 7250 SAS or Telco VLAN is configured using a port that is not in Network mode.
Name: TypeMismatch (96) Type: configurationAlarm (11) Probable cause: serviceSiteTypeMisconfigured (82)	Severity: Critical Object Type (class): Service Domain: service Implicitly cleared (self-clearing): Yes	The alarm is raised when one 5620 SAM service ID is associated with service sites that belong to different service types.
Name: VideoInterfaceDown (794) Type: VideoInterfaceAlarm (72) Probable cause: interfaceDown (32)	Severity: Critical Object Type (class): VideoInterface Domain: service Implicitly cleared (self-clearing): Yes	The alarm is raised when a video interface is operationally down. The alarm clears when the video interface is operationally up.
Name: VLanUplinkDown (1146) Type: VLanUplinkAlarm (89) Probable cause: VLanUplinkDown (852)	Severity: Major Object Type (class): VlanUplink Domain: service Implicitly cleared (self-clearing): Yes	The alarm is raised when a VLAN uplink is operationally down.
Name: VLanUplinkNotCreated (1147) Type: VLanUplinkAlarm (89) Probable cause: VLanUplinkNotCreated (853)	Severity: Major Object Type (class): Service Domain: service Implicitly cleared (self-clearing): Yes	The alarm is raised when an expected VLAN uplink does not exist.

(3 of 3)

Table 3-66 Domain: sitesec

Alarm	Attributes	Description
Name: ManagementAccessFilterMisconfigured (76) Type: configurationAlarm (11) Probable cause: invalidSourcePortIdentifier (61)	Severity: Warning Object Type (class): MacMafEntry, MafEntry Domain: sitesec Implicitly cleared (self-clearing): Yes	The alarm is raised when a MAF is misconfigured.
Name: ManagementAccessFilterMisconfiguredIpv6 (1112) Type: configurationAlarm (11) Probable cause: invalidSourcePortIdentifier (61)	Severity: Warning Object Type (class): MafIPv6Entry Domain: sitesec Implicitly cleared (self-clearing): Yes	The alarm is raised when an IPv6 MAF is misconfigured.

Table 3-67 Domain: snmp

Alarm	Attributes	Description
Name: MediationAuthenticationFailure (75) Type: communicationsAlarm (4) Probable cause: noMediationPolicyFound (62)	Severity: Critical Object Type (class): PollerManager Domain: snmp Implicitly cleared (self-clearing): No	The alarm is raised when an NE has no associated 5620 SAM mediation policy.

Table 3-68 Domain: sonet

Alarm	Attributes	Description
Name: AllTimingReferencesNotQualified (549) Type: communicationsAlarm (4) Probable cause: allTimingReferencesNotQualified (419)	Severity: Major Object Type (class): SiteSync Domain: sonet Implicitly cleared (self-clearing): Yes	The alarm is raised when no timing references on an NE are in the Qualified state.
Name: BITS2NotQualified (1941) Type: communicationsAlarm (4) Probable cause: timingReferenceNotQualified (418)	Severity: Minor Object Type (class): SiteSync Domain: sonet Implicitly cleared (self-clearing): Yes	The alarm is raised when the BITS-2 timing reference on an NE is not in the Qualified state.
Name: BITSNotQualified (547) Type: communicationsAlarm (4) Probable cause: timingReferenceNotQualified (418)	Severity: Minor Object Type (class): SiteSync Domain: sonet Implicitly cleared (self-clearing): Yes	The alarm is raised when the BITS timing reference on an NE is not in the Qualified state.
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm (4) Probable cause: BITSReferenceLossOfSignal (938)	Severity: Minor Object Type (class): SiteSync Domain: sonet Implicitly cleared (self-clearing): Yes	The alarm is raised when the BITS reference on an NE is not qualified due to Loss of Signal.
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm (4) Probable cause: BITSReferenceOutOfFrequency (939)	Severity: Minor Object Type (class): SiteSync Domain: sonet Implicitly cleared (self-clearing): Yes	The alarm is raised when the BITS Reference on an NE is not qualified due to Out of frequency.
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm (4) Probable cause: BITSReferenceOutOfPollInRange (940)	Severity: Minor Object Type (class): SiteSync Domain: sonet Implicitly cleared (self-clearing): Yes	The alarm is raised when the BITS Reference on an NE is not qualified state due to Out of poll in range.
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm (4) Probable cause: timingReferenceNotQualified (418)	Severity: Minor Object Type (class): SiteSync Domain: sonet Implicitly cleared (self-clearing): Yes	The alarm is raised when the External timing reference on an NE is not in the Qualified state.
Name: ReferenceOneLossOfSignal (1953) Type: communicationsAlarm (4) Probable cause: ReferenceOneLossOfSignal (941)	Severity: Minor Object Type (class): SiteSync Domain: sonet Implicitly cleared (self-clearing): Yes	The alarm is raised when the Timing Reference One on an NE is not qualified due to Loss of Signal.

(1 of 2)

Alarm	Attributes	Description
Name: ReferenceOneOutOfFrequency (1954) Type: communicationsAlarm (4) Probable cause: ReferenceOneOutOfFrequency (942)	Severity: Minor Object Type (class): SiteSync Domain: sonet Implicitly cleared (self-clearing): Yes	The alarm is raised when the Timing Reference One on an NE is not qualified due to Out of frequency.
Name: ReferenceOneOutOfPollInRange (1955) Type: communicationsAlarm (4) Probable cause: ReferenceOneOutOfPollInRange (943)	Severity: Minor Object Type (class): SiteSync Domain: sonet Implicitly cleared (self-clearing): Yes	The alarm is raised when the Timing Reference One on an NE is not qualified due to Out of poll in range.
Name: ReferenceTwoLossOfSignal (1956) Type: communicationsAlarm (4) Probable cause: ReferenceTwoLossOfSignal (944)	Severity: Minor Object Type (class): SiteSync Domain: sonet Implicitly cleared (self-clearing): Yes	The alarm is raised when the Timing Reference Two on an NE is not qualified due to Loss of Signal.
Name: ReferenceTwoOutOfFrequency (1957) Type: communicationsAlarm (4) Probable cause: ReferenceTwoOutOfFrequency (945)	Severity: Minor Object Type (class): SiteSync Domain: sonet Implicitly cleared (self-clearing): Yes	The alarm is raised when the Timing Reference Two on an NE is not qualified due to Out of frequency.
Name: ReferenceTwoOutOfPollInRange (1958) Type: communicationsAlarm (4) Probable cause: ReferenceTwoOutOfPollInRange (946)	Severity: Minor Object Type (class): SiteSync Domain: sonet Implicitly cleared (self-clearing): Yes	The alarm is raised when the Timing Reference Two on an NE is not qualified due to Out of poll in range.
Name: SiteSyncDeploymentFailure (589) Type: equipmentAlarm (3) Probable cause: siteSyncFailure (441)	Severity: Major Object Type (class): SiteSync Domain: sonet Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM tries to deploy a value for an object when a transaction that involves the object is in progress from a different context.
Name: TimingHoldover (734) Type: communicationsAlarm (4) Probable cause: timingHoldover (511)	Severity: Major Object Type (class): SiteSync Domain: sonet Implicitly cleared (self-clearing): Yes	The alarm is raised when the timing of an NE is in the Holdover state.
Name: TimingReferenceOneNotQualified (545) Type: communicationsAlarm (4) Probable cause: timingReferenceNotQualified (418)	Severity: Minor Object Type (class): SiteSync Domain: sonet Implicitly cleared (self-clearing): Yes	The alarm is raised when Timing Reference One on an NE is not in the Qualified state.
Name: TimingReferenceTwoNotQualified (546) Type: communicationsAlarm (4) Probable cause: timingReferenceNotQualified (418)	Severity: Minor Object Type (class): SiteSync Domain: sonet Implicitly cleared (self-clearing): Yes	The alarm is raised when Timing Reference Two on an NE is not in the Qualified state.

(2 of 2)

Table 3-69 Domain: sonetequipment

Alarm	Attributes	Description
Name: BerLineSignalDegradation (88) Type: communicationsAlarm (4) Probable cause: berLineSignalDegradation (74)	Severity: Major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports a line signal degradation BER error. The alarm corresponds to the lb2er-sd alarm on an NE.
Name: BerLineSignalFailure (89) Type: communicationsAlarm (4) Probable cause: berLineSignalFailure (75)	Severity: Major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports a line signal degradation BER error. The alarm corresponds to the lb2er-sf alarm on an NE.
Name: LineAlarmIndicationSignal (84) Type: communicationsAlarm (4) Probable cause: lineAlarmIndicationSignal (70)	Severity: Major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports an LAIS error. The alarm corresponds to the lais alarm on an NE.
Name: LineErrorCondition (94) Type: communicationsAlarm (4) Probable cause: lineErrorCondition (80)	Severity: Major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports a line error condition that a remote NE raises because of b1 errors received from the local NE. The alarm corresponds to the lrei alarm on an NE.
Name: LineRemoteDefectIndication (85) Type: communicationsAlarm (4) Probable cause: lineRemoteDefectIndication (71)	Severity: Major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports a line remote defect indication error caused by an LOF, LOC, or LOS condition. The alarm corresponds to the lrdi alarm on an NE.
Name: LossOfClock (83) Type: communicationsAlarm (4) Probable cause: lossOfClock (69)	Severity: Major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports an LOC condition, which causes the NE to set the port Operational State to Down.
Name: RxSectionSynchronizationError (93) Type: communicationsAlarm (4) Probable cause: rxSectionSynchronizationError (79)	Severity: Major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports a section synchronization failure. A section synchronization failure occurs when the S1 byte is inconsistent for eight consecutive frames.
Name: SectionB1Error (87) Type: communicationsAlarm (4) Probable cause: sectionB1Error (73)	Severity: Major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports a section error condition that a remote NE raises because of b1 errors received from the local NE. The alarm corresponds to the lrei alarm on an NE.
Name: SectionLossOfFrame (90) Type: communicationsAlarm (4) Probable cause: sectionLossOfFrame (76)	Severity: Major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports a SLOF error. The alarm corresponds to the slof alarm on an NE.

(1 of 3)

Alarm	Attributes	Description
Name: SectionLossOfSignal (91) Type: communicationsAlarm (4) Probable cause: sectionLossOfSignal (77)	Severity: Major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports a SLOS error. The alarm corresponds to the slos alarm on an NE.
Name: SectionS1Failure (86) Type: communicationsAlarm (4) Probable cause: sectionS1Failure (72)	Severity: Major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports a section synchronization failure. A section synchronization failure occurs when the S1 byte is inconsistent for eight consecutive frames.
Name: SonetPathAlarmIndicationSignal (129) Type: communicationsAlarm (4) Probable cause: pathAlarmIndicationSignal (63)	Severity: Major Object Type (class): SonetChannelMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports a PAIS error. The alarm corresponds to the pais alarm on an NE.
Name: SonetPathB3Error (132) Type: communicationsAlarm (4) Probable cause: pathB3Error (66)	Severity: Major Object Type (class): SonetChannelMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports a path error condition because of b3 errors. The alarm corresponds to the prei alarm on an NE.
Name: SonetPathLossOfCodegroupDelineationError (248) Type: communicationsAlarm (4) Probable cause: pathLossOfCodegroupDelineationError (185)	Severity: Major Object Type (class): SonetChannelMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports a PLCD error. The alarm corresponds to the plcd alarm on an NE.
Name: SonetPathLossOfPointer (130) Type: communicationsAlarm (4) Probable cause: pathLossOfPointer (64)	Severity: Major Object Type (class): SonetChannelMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports a PLOP error. The alarm corresponds to the plop alarm on an NE.
Name: SonetPathPayloadMismatch (133) Type: communicationsAlarm (4) Probable cause: pathPayloadMismatch (67)	Severity: Major Object Type (class): SonetChannelMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports a PPLM error on a channel, after which the channel is set operationally down. The alarm corresponds to the pplm alarm on an NE.
Name: SonetPathRemoteB3Error (134) Type: communicationsAlarm (4) Probable cause: pathRemoteB3Error (68)	Severity: Major Object Type (class): SonetChannelMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports a path error condition that a remote NE raises because of b3 errors received from the local NE. The alarm corresponds to the prei alarm on an NE.
Name: SonetPathRemoteDefectIndication (131) Type: communicationsAlarm (4) Probable cause: pathRemoteDefectIndication (65)	Severity: Major Object Type (class): SonetChannelMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports a remote PAIS error. The alarm corresponds to the pais alarm on an NE.

(2 of 3)

Alarm	Attributes	Description
Name: SonetPathUnequippedPathError (143) Type: communicationsAlarm (4) Probable cause: pathUnequippedPathError (114)	Severity: Major Object Type (class): SonetChannelMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports a path unequipped error. The alarm corresponds to the puneq alarm on an NE.
Name: SonetSDHLoopback (407) Type: configurationAlarm (11) Probable cause: sonetSDHLoopback (303)	Severity: Warning Object Type (class): SonetPortSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): No	The alarm is raised when a loopback test is provisioned on a SONET/SDH port.
Name: TxSectionSynchronizationError (92) Type: communicationsAlarm (4) Probable cause: txSectionSynchronizationError (78)	Severity: Major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when a SONET port reports an SS1F error. The alarm corresponds to the ss1f alarm on an NE.

(3 of 3)

Table 3-70 Domain: srrp

Alarm	Attributes	Description
Name: DualMaster (420) Type: configurationAlarm (11) Probable cause: dualMaster (313)	Severity: Major Object Type (class): Instance Domain: srrp Implicitly cleared (self-clearing): No	The alarm is raised when the local and remote SRRP instances are in the master state.
Name: InstanceDown (284) Type: configurationAlarm (11) Probable cause: instanceDown (216)	Severity: Major Object Type (class): Instance Domain: srrp Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects that an SRRP instance is operationally down.
Name: InstanceIdMismatch (416) Type: configurationAlarm (11) Probable cause: instanceIdMismatch (309)	Severity: Major Object Type (class): Instance Domain: srrp Implicitly cleared (self-clearing): No	The alarm is raised when a local SRRP SAP is backed up by a different SRRP instance on a remote peer.
Name: RedundantIfMismatch (419) Type: configurationAlarm (11) Probable cause: redundantIfNotProperlyPaired (312)	Severity: Major Object Type (class): Instance Domain: srrp Implicitly cleared (self-clearing): No	The alarm is raised when the local and remote redundant interfaces are not correctly paired.
Name: SapMismatch (417) Type: configurationAlarm (11) Probable cause: remoteSapMismatch (310)	Severity: Major Object Type (class): Instance Domain: srrp Implicitly cleared (self-clearing): No	The alarm is raised when the SRRP SAPs on the local interface do not match the SRRP SAPs on the remote interface.
Name: SapTagMismatch (418) Type: configurationAlarm (11) Probable cause: remoteSyncTagMismatch (311)	Severity: Major Object Type (class): Instance Domain: srrp Implicitly cleared (self-clearing): No	The alarm is raised when the tag of a local SAP does not match the tag of a remote SAP.

(1 of 2)

Alarm	Attributes	Description
Name: SubnetMismatch (415) Type: configurationAlarm (11) Probable cause: ipAddressListMismatch (308)	Severity: Major Object Type (class): Instance Domain: srrp Implicitly cleared (self-clearing): Yes	The alarm is raised when the IP address list received from the master does not match the local IP address list.

(2 of 2)

Table 3-71 Domain: subscrident

Alarm	Attributes	Description
Name: backupScriptInUse (274) Type: configurationAlarm (11) Probable cause: backupInUse (206)	Severity: Major Object Type (class): Policy Domain: subscrident Implicitly cleared (self-clearing): Yes	The alarm is raised when the primary subscriber identification script is operationally down, but one of the other scripts is operationally up.
Name: noFunctioningScript (275) Type: configurationAlarm (11) Probable cause: primaryBackupDown (207)	Severity: Critical Object Type (class): Policy Domain: subscrident Implicitly cleared (self-clearing): Yes	The alarm is raised when all subscriber identification scripts are operationally down.
Name: scriptBackupLost (273) Type: configurationAlarm (11) Probable cause: backupDown (205)	Severity: Warning Object Type (class): Policy Domain: subscrident Implicitly cleared (self-clearing): Yes	The alarm is raised when the primary subscriber identification script URL is operationally up, but a lower-priority script or URL is operationally down.

Table 3-72 Domain: svq

Alarm	Attributes	Description
Name: TodSuiteAssignmentFailure (312) Type: todSuiteAlarm (35) Probable cause: assignmentFailure (242)	Severity: Minor Object Type (class): AggregationScheduler Domain: svq Implicitly cleared (self-clearing): No	The alarm is raised when an object fails to perform the action specified in a Time of Day suite.

Table 3-73 Domain: svt

Alarm	Attributes	Description
Name: FrameSizeProblem (37) Type: configurationAlarm (11) Probable cause: frameSizeProblem (33)	Severity: Critical Object Type (class): SdpBinding Domain: svt Implicitly cleared (self-clearing): Yes	The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.

(1 of 3)

Alarm	Attributes	Description
Name: HashLabelMismatch (1113) Type: configurationAlarm (11) Probable cause: hashLabelMismatch (826)	Severity: Warning Object Type (class): SdpBinding Domain: svt Implicitly cleared (self-clearing): Yes	The alarm is raised when an SDP binding hash label is enabled and the return SDP binding hash label is disabled. The receiving site drops the data packets as a result.
Name: IgmpSnpgGrpDroppedLimitExceeded (392) Type: SdpBindingAlarm (30) Probable cause: igmpSnpgGrpMaxNbrGrpsReached (292)	Severity: Warning Object Type (class): SdpBindingIgmpSnpgCfg Domain: svt Implicitly cleared (self-clearing): No	The alarm is raised when an IGMP group is removed from an SDP binding because the number of allowed IGMP groups specified by sdpBndIgmpSnpgCfgMaxNbrGrps is reached.
Name: IgmpSnpgSrcDroppedLimitExceeded (735) Type: SdpBindingAlarm (30) Probable cause: igmpSnpgGrpMaxNbrSrcsReached (512)	Severity: Warning Object Type (class): SdpBindingIgmpSnpgCfg Domain: svt Implicitly cleared (self-clearing): No	The alarm is raised when an IGMP source is removed from an SDP binding because the number of allowed IGMP sources specified by sdpBndIgmpSnpgCfgMaxNbrSrcs is reached.
Name: KeepAliveProblem (100) Type: oamAlarm (18) Probable cause: keepAliveFailed (86)	Severity: Warning Object Type (class): Tunnel Domain: svt Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.
Name: LabelProblem (98) Type: CircuitAlarm (17) Probable cause: labelProblem (84)	Severity: Critical Object Type (class): SdpBinding Domain: svt Implicitly cleared (self-clearing): Yes	The alarm is raised when an ingress or an egress label is missing.
Name: McacPolicyDropped (341) Type: communicationsAlarm (4) Probable cause: igmpGroupOnSdpBindDropped (265)	Severity: Major Object Type (class): SdpBindingIgmpSnpgCfg Domain: svt Implicitly cleared (self-clearing): No	The alarm is raised when an IGMP group is dropped because a multicast CAC policy is applied to an SDP binding.
Name: SdpBindingDown (221) Type: SdpBindingAlarm (30) Probable cause: SdpBindingNotReady (166)	Severity: Critical Object Type (class): SdpBinding Domain: svt Implicitly cleared (self-clearing): Yes	The alarm is raised when an SDP binding has an Operational State other than Up, and the Administrative State is Up.
Name: SdpBindingMisconfigured (293) Type: SdpBindingAlarm (30) Probable cause: returnSdpBindingTypeMismatch (224)	Severity: Critical Object Type (class): SdpBinding Domain: svt Implicitly cleared (self-clearing): Yes	The alarm is raised when the return SDP binding type does not match the originating SDP binding type, for example, when the return SDP binding is spoke and the originating SDP binding is mesh.
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm (17) Probable cause: SdpTunnelNotReady (167)	Severity: Critical Object Type (class): SdpBinding Domain: svt Implicitly cleared (self-clearing): Yes	The alarm is raised when an SDP binding tunnel has an Operational State other than Up, and the Administrative State is Up.
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm (18) Probable cause: networkDegradation (204)	Severity: Major Object Type (class): Tunnel Domain: svt Implicitly cleared (self-clearing): Yes	The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.

(2 of 3)

Alarm	Attributes	Description
Name: TestThresholdExceededAlarm2 (1918) Type: oamAlarm (18) Probable cause: networkDegradation (204)	Severity: Major Object Type (class): SdpBinding Domain: svt Implicitly cleared (self-clearing): Yes	The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.
Name: TunnelAdministrativelyDown (523) Type: pathAlarm (12) Probable cause: tunnelAdministrativelyDown (333)	Severity: Minor Object Type (class): Tunnel Domain: svt Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.
Name: TunnelDown (30) Type: pathAlarm (12) Probable cause: tunnelDown (23)	Severity: Critical Object Type (class): Tunnel Domain: svt Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.
Name: TunnelOverbooked (590) Type: resourceAlarm (28) Probable cause: tunnelOverbooked (442)	Severity: Warning Object Type (class): Tunnel Domain: svt Implicitly cleared (self-clearing): No	The alarm is raised when the allocated SDP binding bandwidth specified by sdpBookedBandwidth exceeds the sdpMaxBookableBandwidth value.

(3 of 3)

Table 3-74 Domain: sw

Alarm	Attributes	Description
Name: BootableConfigBackupFailed (103) Type: configurationAlarm (11) Probable cause: fileTransferFailure (89)	Severity: Major Object Type (class): BackupRestoreManager Domain: sw Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm (11) Probable cause: fileTransferFailure (89)	Severity: Major Object Type (class): BackupRestoreManager Domain: sw Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.
Name: BootEnvironmentSyncFailed (101) Type: equipmentAlarm (3) Probable cause: bootEnvironmentSyncFailed (87)	Severity: Critical Object Type (class): SoftwareUpgradeManager Domain: sw Implicitly cleared (self-clearing): Yes	The alarm is raised when the synchronization of one or more system initialization files between the active and standby CPM cards fails. See the 7750 SR OS System Guide for more information.
Name: certifyFailureAlarm (533) Type: softwareAlarm (19) Probable cause: certifyFailureAlarm (402)	Severity: Major Object Type (class): SoftwareControlModule Domain: sw Implicitly cleared (self-clearing): No	The alarm is raised when the software certification process on an NE fails.
Name: ConfigFileSyncFailed (102) Type: equipmentAlarm (3) Probable cause: configFileSyncFailed (88)	Severity: Critical Object Type (class): SoftwareUpgradeManager Domain: sw Implicitly cleared (self-clearing): Yes	The alarm is raised when the configuration file synchronization between the active and standby CPM cards fails.

(1 of 3)

Alarm	Attributes	Description
Name: DataLossAlarm (148) Type: storageAlarm (25) Probable cause: dataLoss (122)	Severity: Major Object Type (class): AccountingStatsRetrievalManager Domain: sw Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM receives the tmnxLogAccountingDataLoss trap, which is sent when a statistics collection interval ends while an NE is writing data to an accounting file. The statistics collection for the interval stops immediately, and collection for the next interval begins. The accounting statistics file for the interrupted collection contains an incomplete data set as a result.
Name: HardwareBootFailure (108) Type: softwareAlarm (19) Probable cause: softwareBootProblemDueToHardwareIssues (92)	Severity: Critical Object Type (class): CardSoftware Domain: sw Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE fails to boot because of a hardware problem.
Name: PrimaryImageBootFailure (191) Type: configurationAlarm (11) Probable cause: bootOptionFileMisconfigured (150)	Severity: Warning Object Type (class): CardSoftware Domain: sw Implicitly cleared (self-clearing): Yes	The alarm is raised when the primary software image specified in an NE BOF is unusable.
Name: restoreFailureAlarm (535) Type: softwareAlarm (19) Probable cause: restoreFailureAlarm (404)	Severity: Major Object Type (class): SoftwareControlModule Domain: sw Implicitly cleared (self-clearing): No	The alarm is raised when the software restore process on an NE fails.
Name: SaveConfigFailed (105) Type: configurationAlarm (11) Probable cause: fileAccessError (90)	Severity: Major Object Type (class): BackupRestoreManager Domain: sw Implicitly cleared (self-clearing): Yes	The alarm is raised when the admin save command on an NE fails.
Name: SoftwareBootFailure (107) Type: softwareAlarm (19) Probable cause: softwareBootProblem (91)	Severity: Major Object Type (class): CardSoftware Domain: sw Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE fails to boot because of a software problem.
Name: SoftwareDownloading (109) Type: softwareAlarm (19) Probable cause: softwareDownloading (93)	Severity: Warning Object Type (class): CardSoftware Domain: sw Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE begins to download software to a IOM or CPM card.
Name: SoftwareInitialized (111) Type: softwareAlarm (19) Probable cause: softwareInitialized (95)	Severity: Warning Object Type (class): CardSoftware Domain: sw Implicitly cleared (self-clearing): Yes	The alarm is raised when software initialization on an IOM or CPM card completes.
Name: SoftwareInitializing (110) Type: softwareAlarm (19) Probable cause: softwareInitializing (94)	Severity: Warning Object Type (class): CardSoftware Domain: sw Implicitly cleared (self-clearing): Yes	The alarm is raised when software initialization on an IOM or CPM card begins.

(2 of 3)

Alarm	Attributes	Description
Name: SoftwareUpgradeFailed (106) Type: configurationAlarm (11) Probable cause: fileAccessError (90)	Severity: Major Object Type (class): SoftwareUpgradeManager Domain: sw Implicitly cleared (self-clearing): No	The alarm is raised when an NE software upgrade using the 5620 SAM fails.
Name: StatsRetrieveFailed (244) Type: configurationAlarm (11) Probable cause: fileTransferFailure (89)	Severity: Major Object Type (class): AccountingStatsRetrievalManager Domain: sw Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM cannot transfer an accounting file from an NE.
Name: synchroFailureAlarm (534) Type: softwareAlarm (19) Probable cause: synchroFailureAlarm (403)	Severity: Major Object Type (class): SoftwareControlModule Domain: sw Implicitly cleared (self-clearing): No	The alarm is raised when the flash card synchronization on an NE fails.
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm (11) Probable cause: versionMismatch (405)	Severity: Major Object Type (class): BackupRestoreManager Domain: sw Implicitly cleared (self-clearing): Yes	The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.

(3 of 3)

Table 3-75 Domain: tca

Alarm	Attributes	Description
Name: ThresholdCrossingAlarm (14) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Variable or indeterminate Object Type (class): TCAPolicy Domain: tca Implicitly cleared (self-clearing): No	The alarm is raised when a monitored object statistics-counter value exceeds a threshold value in the associated statistics policy.

Table 3-76 Domain: tdmequipment

Alarm	Attributes	Description
Name: DS1E1AlarmIndicationSignal (112) Type: communicationsAlarm (4) Probable cause: alarmIndicationSignal (96)	Severity: Major Object Type (class): DS1E1ChannelSpecifics Domain: tdmequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE reports that a specific DS1 or E1 channel has an AIS alarm condition.
Name: DS1E1Loopback (409) Type: configurationAlarm (11) Probable cause: ds1e1Loopback (305)	Severity: Warning Object Type (class): DS1E1ChannelSpecifics Domain: tdmequipment Implicitly cleared (self-clearing): No	The alarm is raised when an NE reports that a specific DS1 or E1 channel has a loopback alarm condition.

(1 of 3)

Alarm	Attributes	Description
Name: DS1E1Looped (126) Type: communicationsAlarm (4) Probable cause: farEndLoopback (102)	Severity: Major Object Type (class): DS1E1ChannelSpecifics Domain: tdmequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE reports that a specific DS1 or E1 channel has a remote loopback alarm condition.
Name: DS1E1LossOfSignal (124) Type: communicationsAlarm (4) Probable cause: lossOfSignal (99)	Severity: Major Object Type (class): DS1E1ChannelSpecifics Domain: tdmequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE reports that a specific DS1 or E1 channel has an LOS alarm condition.
Name: DS1E1OutOfFrame (125) Type: communicationsAlarm (4) Probable cause: outOfFrame (100)	Severity: Major Object Type (class): DS1E1ChannelSpecifics Domain: tdmequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE reports that a specific DS1 or E1 channel has an OOF alarm condition.
Name: DS1E1ResourceAvailabilityIndicator (114) Type: communicationsAlarm (4) Probable cause: resourceAvailabilityIndicator (98)	Severity: Major Object Type (class): DS1E1ChannelSpecifics Domain: tdmequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE reports that a specific DS1 or E1 channel has an RAI alarm condition.
Name: DS1E1SignalDegradation (500) Type: communicationsAlarm (4) Probable cause: signalDegradation (386)	Severity: Major Object Type (class): DS1E1ChannelSpecifics Domain: tdmequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SD alarm condition.
Name: DS1E1SignalFailure (501) Type: communicationsAlarm (4) Probable cause: signalFailure (387)	Severity: Major Object Type (class): DS1E1ChannelSpecifics Domain: tdmequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SF alarm condition.
Name: DS3E3AlarmIndicationSignal (115) Type: communicationsAlarm (4) Probable cause: alarmIndicationSignal (96)	Severity: Major Object Type (class): DS3E3ChannelSpecifics Domain: tdmequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE reports that a specific DS3 or E3 channel has an AIS alarm condition.
Name: DS3E3Loopback (408) Type: configurationAlarm (11) Probable cause: ds3e3Loopback (304)	Severity: Warning Object Type (class): DS3E3ChannelSpecifics Domain: tdmequipment Implicitly cleared (self-clearing): No	The alarm is raised when an NE reports that a specific DS3 or E3 channel has a loopback alarm condition.
Name: DS3E3Looped (120) Type: communicationsAlarm (4) Probable cause: farEndLoopback (102)	Severity: Major Object Type (class): DS3E3ChannelSpecifics Domain: tdmequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE reports that a specific DS3 or E3 channel has a remote loopback alarm condition.

(2 of 3)

Alarm	Attributes	Description
Name: DS3E3LossOfSignal (116) Type: communicationsAlarm (4) Probable cause: lossOfSignal (99)	Severity: Major Object Type (class): DS3E3ChannelSpecifics Domain: tdmequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE reports that a specific DS3 or E3 channel has an LOS alarm condition.
Name: DS3E3OutOfFrame (117) Type: communicationsAlarm (4) Probable cause: outOfFrame (100)	Severity: Major Object Type (class): DS3E3ChannelSpecifics Domain: tdmequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE reports that a specific DS3 or E3 channel has an OOF alarm condition.
Name: DS3E3ResourceAvailability (119) Type: communicationsAlarm (4) Probable cause: resourceAvailabilityIndicator (98)	Severity: Major Object Type (class): DS3E3ChannelSpecifics Domain: tdmequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE reports that a specific DS3 or E3 channel has an RAI alarm condition.
Name: SerialChannelLoopback (807) Type: configurationAlarm (11) Probable cause: serialChannelLoopback (573)	Severity: Warning Object Type (class): SerialChannelSpecifics Domain: tdmequipment Implicitly cleared (self-clearing): No	The alarm is raised when an NE reports that a serial channel has a loopback alarm condition.
Name: SerialChannelOutOfFrame (808) Type: communicationsAlarm (4) Probable cause: outOfFrame (100)	Severity: Major Object Type (class): SerialChannelSpecifics Domain: tdmequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE reports that a serial channel has an OOF alarm condition.
Name: SerialChannelRemoteAlarmIndication (809) Type: communicationsAlarm (4) Probable cause: remoteAlarmIndication (574)	Severity: Major Object Type (class): SerialChannelSpecifics Domain: tdmequipment Implicitly cleared (self-clearing): Yes	The alarm is raised when an NE reports that a serial channel has an RAI condition.
Name: VoiceChannelLoopback (1148) Type: configurationAlarm (11) Probable cause: voiceChannelLoopback (854)	Severity: Warning Object Type (class): VoiceChannelSpecifics Domain: tdmequipment Implicitly cleared (self-clearing): No	The alarm is raised when an NE reports that a voice channel has a loopback alarm condition.

(3 of 3)

Table 3-77 Domain: template

Alarm	Attributes	Description
Name: ChildTemplateInvalid (193) Type: configurationAlarm (11) Probable cause: referencedObjectInvalid (152)	Severity: Major Object Type (class): TemplateBinding Domain: template Implicitly cleared (self-clearing): Yes	The alarm is raised when a child template in a template binding is invalid. The alarm is deprecated in the 5620 SAM, Release 6.0 and later.

(1 of 2)

Alarm	Attributes	Description
Name: DependentObjectDeleted (192) Type: configurationAlarm (11) Probable cause: referencedObjectGone (151)	Severity: Major Object Type (class): Template Domain: template Implicitly cleared (self-clearing): Yes	The alarm is raised when an object referenced by a template cannot be found. The alarm is deprecated in the 5620 SAM, Release 6.0 and later.
Name: ParentTemplateInvalid (194) Type: configurationAlarm (11) Probable cause: referencedObjectInvalid (152)	Severity: Major Object Type (class): TemplateBinding Domain: template Implicitly cleared (self-clearing): Yes	The alarm is raised when a parent template in a template binding is invalid. The alarm is deprecated in the 5620 SAM, Release 6.0 and later.

(2 of 2)

Table 3-78 Domain: trapmapper

Alarm	Attributes	Description
Name: TrapMapperQueueFull (797) Type: queueFull (73) Probable cause: trapRateTooHigh (564)	Severity: Critical Object Type (class): TrapMapperManager Domain: trapmapper Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM detects that the queue for traps that are to be mapped to alarms is full. Until queue space is available, the 5620 SAM drops traps that are to be mapped to alarms.

Table 3-79 Domain: tunnelmgmt

Alarm	Attributes	Description
Name: PacingInProgressWarning (737) Type: configurationAlarm (11) Probable cause: noUpdatesDueToPacingInProgress (514)	Severity: Warning Object Type (class): TopologyRule Domain: tunnelmgmt Implicitly cleared (self-clearing): Yes	The alarm is raised when tunnel creation or deletion is not performed after a member is added or removed from a rule group because topology rule pacing is in progress. When this occurs, the Reapply and Delete Unused operations must be performed manually when the pacing is complete. The alarm clears after a Reapply operation is performed.
Name: TopologyRuleExecutionError (365) Type: configurationAlarm (11) Probable cause: ruleErrorOrRuleEngineError (262)	Severity: Major Object Type (class): TopologyRule Domain: tunnelmgmt Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM cannot execute a topology rule or when rule execution generates an error. Rule execution is the process that determines which tunnel elements require creation, modification, or deletion. The alarm typically indicates that the rule is misconfigured.
Name: TunnelElementCreationError (366) Type: configurationAlarm (11) Probable cause: unableToCreateTunnelElement (263)	Severity: Major Object Type (class): TopologyRule Domain: tunnelmgmt Implicitly cleared (self-clearing): No	The alarm is raised when the creation of a missing tunnel element fails.

(1 of 2)

Alarm	Attributes	Description
Name: TunnelElementDeleteError (367) Type: configurationAlarm (11) Probable cause: tunnelElementInUse (264)	Severity: Major Object Type (class): TopologyRule Domain: tunnelmgmt Implicitly cleared (self-clearing): No	The alarm is raised when the deletion of an obsolete or unused tunnel element fails.
Name: TunnelElementInUseWarning (368) Type: configurationAlarm (11) Probable cause: tunnelElementInUse (264)	Severity: Warning Object Type (class): TopologyRule Domain: tunnelmgmt Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM does not attempt to delete an obsolete or unused tunnel element because the element is in use by another object.

(2 of 2)

Table 3-80 Domain: vlan

Alarm	Attributes	Description
Name: IfVlanSubTypeConflict (213) Type: configurationAlarm (11) Probable cause: topologyMisconfigured (81)	Severity: Major Object Type (class): L2AccessInterface Domain: vlan Implicitly cleared (self-clearing): Yes	The alarm is raised when more than one type of VLAN service is configured with the same VLAN ID. The alarm is raised against an L2 access interface.
Name: ManagementVlanConflict (215) Type: configurationAlarm (11) Probable cause: topologyMisconfigured (81)	Severity: Warning Object Type (class): Vlan Domain: vlan Implicitly cleared (self-clearing): Yes	The alarm is raised when a management VLAN ID is in use by another service type.
Name: SapVlanSubTypeConflict (290) Type: configurationAlarm (11) Probable cause: topologyMisconfigured (81)	Severity: Warning Object Type (class): Site Domain: vlan Implicitly cleared (self-clearing): No	The alarm is raised when a SAP resynchronization indicates that the VLAN subtype of the SAP is different from the site subtype. The alarm information includes the ID of the associated port.
Name: SiteManagementVlanConflict (223) Type: configurationAlarm (11) Probable cause: topologyMisconfigured (81)	Severity: Warning Object Type (class): Site Domain: vlan Implicitly cleared (self-clearing): Yes	The alarm is raised when the management VLAN ID is used for another type of service.
Name: SiteVlanSubTypeConflict (224) Type: configurationAlarm (11) Probable cause: topologyMisconfigured (81)	Severity: Major Object Type (class): Site Domain: vlan Implicitly cleared (self-clearing): Yes	The alarm is raised when more than one type of VLAN service has the same VLAN ID. The alarm is raised against a site.
Name: VlanSubTypeConflict (227) Type: configurationAlarm (11) Probable cause: topologyMisconfigured (81)	Severity: Major Object Type (class): Vlan Domain: vlan Implicitly cleared (self-clearing): Yes	The alarm is raised when more than one type of VLAN service has the same VLAN ID. The alarm is raised against a service.

Table 3-81 Domain: vll

Alarm	Attributes	Description
Name: CesBfrOverrun (448) Type: communicationsAlarm (4) Probable cause: bufferOverrun (322)	Severity: Major Object Type (class): VllCesInterfaceSpecifics Domain: vll Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects a jitter buffer overrun.
Name: CesBfrUnderrun (449) Type: communicationsAlarm (4) Probable cause: bufferOverrun (322)	Severity: Major Object Type (class): VllCesInterfaceSpecifics Domain: vll Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects a jitter buffer underrun.
Name: CesMalformedPkts (446) Type: communicationsAlarm (4) Probable cause: malformedPackets (320)	Severity: Major Object Type (class): VllCesInterfaceSpecifics Domain: vll Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects one or more malformed packets.
Name: CesPktLoss (447) Type: communicationsAlarm (4) Probable cause: lossOfPacket (321)	Severity: Major Object Type (class): VllCesInterfaceSpecifics Domain: vll Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects a packet loss.
Name: CesRmtPktLoss (450) Type: communicationsAlarm (4) Probable cause: farEndLossOfPacket (323)	Severity: Minor Object Type (class): VllCesInterfaceSpecifics Domain: vll Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects a remote packet loss.
Name: CesRmtRdi (452) Type: configurationAlarm (11) Probable cause: farEndRdi (325)	Severity: Minor Object Type (class): VllCesInterfaceSpecifics Domain: vll Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM detects a remote RDI.
Name: CesRmtTdmFault (451) Type: configurationAlarm (11) Probable cause: tdmFarEndFault (324)	Severity: Minor Object Type (class): VllCesInterfaceSpecifics Domain: vll Implicitly cleared (self-clearing): No	The alarm is raised when the 5620 SAM detects a remote TDM fault.
Name: CesStrayPkts (445) Type: communicationsAlarm (4) Probable cause: strayPackets (319)	Severity: Minor Object Type (class): VllCesInterfaceSpecifics Domain: vll Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects received stray packets.
Name: EncapsulationTypeIncompatible (250) Type: configurationAlarm (11) Probable cause: sapEncapsulationTypeIncompatible (189)	Severity: Major Object Type (class): Vll Domain: vll Implicitly cleared (self-clearing): No	The alarm is raised when the encapsulation types of two SAPs in the same Ipipe are mismatched.

(1 of 2)

Alarm	Attributes	Description
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm (18) Probable cause: networkDegradation (204)	Severity: Major Object Type (class): Vll Domain: vll Implicitly cleared (self-clearing): Yes	The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.

(2 of 2)

Table 3-82 Domain: vpls

Alarm	Attributes	Description
Name: BgpAdVplsIdDiscoveryError (572) Type: serviceAlarm (16) Probable cause: bgpAdVplsIdInconsistent (439)	Severity: Major Object Type (class): AbstractSite Domain: vpls Implicitly cleared (self-clearing): Yes	The alarm is raised when the VPLS ID of a discovered VPLS instance is ambiguous.
Name: BgpAdVplsIdMisconfiguration (570) Type: configurationAlarm (11) Probable cause: bgpAdVplsIdInconsistent (439)	Severity: Major Object Type (class): AbstractVpls Domain: vpls Implicitly cleared (self-clearing): Yes	The alarm is raised when the VPLS ID of a site does not match the VPLS ID of the other sites in the service.
Name: BWUtilizationExceededOnLink (1115) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Major Object Type (class): AbstractVpls Domain: vpls Implicitly cleared (self-clearing): Yes	The alarm is raised when the per-CoS or overall bandwidth utilization on a physical link that is used by a VLAN uplink exceeds the configured threshold.
Name: BWUtilizationExceededOnTunnel (812) Type: thresholdCrossed (6) Probable cause: thresholdCrossed (12)	Severity: Major Object Type (class): Vpls Domain: vpls Implicitly cleared (self-clearing): Yes	The alarm is raised when the per-CoS or overall bandwidth utilization on a tunnel exceeds the configured threshold.
Name: EndpointMacLimitReached (444) Type: resourceAlarm (28) Probable cause: resourceLimitReached (131)	Severity: Warning Object Type (class): Endpoint Domain: vpls Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM receives the svcEndpointMacLimitAlarmRaised trap from an NE, which indicates that the number of MAC addresses stored in the FDB for the endpoint exceeds the high watermark for the site FIB. The number of MAC addresses includes the static MAC addresses on the endpoint and the learned MAC addresses in the spoke SDPs that are associated with the endpoint. The alarm clears when the 5620 SAM receives the svcEndpointMacLimitAlarmCleared trap from the NE.
Name: ForceQTagForwardingMisconfiguration (813) Type: configurationAlarm (11) Probable cause: forceQTagForwardingInconsistent (576)	Severity: Warning Object Type (class): AbstractVpls Domain: vpls Implicitly cleared (self-clearing): Yes	The alarm is raised when two I-sites in a service use different Force Q Tag Forwarding values.

(1 of 3)

Alarm	Attributes	Description
Name: IgmpSnpgGrpDroppedLimitExceeded (392) Type: AccessInterfaceAlarm (32) Probable cause: igmpSnpgGrpMaxNbrGrpsReached (292)	Severity: Warning Object Type (class): L2AccessInterfaceIgmpSnpgCfg Domain: vpls Implicitly cleared (self-clearing): No	The alarm is raised when an IGMP group is removed from a SAP because the number of allowed IGMP groups specified by sapIgmpSnpgCfgMaxNbrGrps is reached.
Name: IgmpSnpgSrcDroppedLimitExceeded (735) Type: AccessInterfaceAlarm (32) Probable cause: igmpSnpgGrpMaxNbrSrcsReached (512)	Severity: Warning Object Type (class): L2AccessInterfaceIgmpSnpgCfg Domain: vpls Implicitly cleared (self-clearing): No	The alarm is raised when an IGMP source is removed from a SAP because the number of allowed IGMP sources specified by sapIgmpSnpgCfgMaxNbrGrps is reached.
Name: InterfaceDown (36) Type: configurationAlarm (11) Probable cause: interfaceDown (32)	Severity: Major Object Type (class): L2ManagementInterface Domain: vpls Implicitly cleared (self-clearing): Yes	The alarm is raised when an L2 management interface has an Operational State of Down, and the associated VPLS site has an Administrative State of Up.
Name: IsidMisconfiguration (592) Type: configurationAlarm (11) Probable cause: isidInconsistent (446)	Severity: Warning Object Type (class): AbstractVpls Domain: vpls Implicitly cleared (self-clearing): Yes	The alarm is raised when service sites use inconsistent I-SID values for a PBB backbone. The alarm is raised against a VPLS or M-VPLS service.
Name: MacPinningViolation (443) Type: serviceAlarm (16) Probable cause: macAddressPinned (348)	Severity: Warning Object Type (class): AbstractSite Domain: vpls Implicitly cleared (self-clearing): No	The alarm is raised when an attempt is made to assign a pinned MAC address to another L2 access interface or spoke SDP binding in an M-VPLS or VPLS.
Name: McacPolicyDropped (341) Type: communicationsAlarm (4) Probable cause: igmpGroupOnSapDropped (246)	Severity: Major Object Type (class): L2AccessInterfaceIgmpSnpgCfg Domain: vpls Implicitly cleared (self-clearing): No	The alarm is raised when an IGMP group is removed from a SAP because a multicast CAC policy is applied.
Name: MFibTableSizeLimitReached (190) Type: resourceAlarm (28) Probable cause: resourceLimitReached (131)	Severity: Warning Object Type (class): AbstractBSite, AbstractTlsSite Domain: vpls Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM receives a svcTlsMfibTableFullAlarmRaised trap for a VPLS site. The alarm clears when the 5620 SAM receives a svcTlsMfibTableFullAlarmCleared trap for the site.
Name: MissSpokeConfiguration (218) Type: configurationAlarm (11) Probable cause: missSpokeConfiguration (172)	Severity: Warning Object Type (class): AbstractVpls Domain: vpls Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects a spoke SDP binding between two sites in one M-VPLS or VPLS.The alarm is not raised by the 5620 SAM, Release 4.0 or later.
Name: MldSnpgGrpDroppedLimitExceeded (537) Type: AccessInterfaceAlarm (32) Probable cause: mldSnpgGrpMaxNbrGrpsReached (406)	Severity: Warning Object Type (class): L2AccessInterfaceMldSnpgCfg Domain: vpls Implicitly cleared (self-clearing): No	The alarm is raised when a SAP drops an MLD group because the configurable maximum number of MLD groups on the SAP is reached.
Name: msapCreationFailure (740) Type: ConfigurationAlarm (15) Probable causes: • creationFailure (515) • radiusAuthFailed (516)	Severity: Warning Object Type (class): L2AccessInterface Domain: vpls Implicitly cleared (self-clearing): No	The alarm is raised when an NE notifies the 5620 SAM that it cannot create an MSAP.

(2 of 3)

Alarm	Attributes	Description
Name: MvrConfiguredFromVplsNotExist (219) Type: configurationAlarm (11) Probable cause: MvrConfiguredFromVplsNotExist (164)	Severity: Warning Object Type (class): L2AccessInterfaceMldMvrCfg, L2AccessInterfaceMvrCfg Domain: vpls Implicitly cleared (self-clearing): Yes	The alarm is raised when an MVR source is an MVR VPLS that does not exist. The alarm clears when the MVR VPLS is created.
Name: MvrConfiguredProxySapNotExist (220) Type: configurationAlarm (11) Probable cause: MvrConfiguredProxySapNotExist (165)	Severity: Warning Object Type (class): L2AccessInterfaceMldMvrCfg, L2AccessInterfaceMvrCfg Domain: vpls Implicitly cleared (self-clearing): Yes	The alarm is raised when a configured MVR proxy SAP does not exist. The alarm clears when the proxy SAP is created.
Name: NeighborLoss (188) Type: communicationsAlarm (4) Probable cause: NeighborConnectionLost (148)	Severity: Warning Object Type (class): InterfacePimSnooping Domain: vpls Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects a loss of connection to a PIM neighbor.
Name: PbbSiteMisconfiguration (571) Type: configurationAlarm (11) Probable cause: includeBothBAndISite (440)	Severity: Warning Object Type (class): AbstractVpls Domain: vpls Implicitly cleared (self-clearing): Yes	The alarm is raised when a VPLS contains a B-Site and an I-Site.
Name: SdpMldSnpgGrpDroppedLimitExceeded (738) Type: SdpBindingAlarm (30) Probable cause: igmpSnpgGrpMaxNbrGrpsReached (292)	Severity: Warning Object Type (class): SdpBindingMldSnpgCfg Domain: vpls Implicitly cleared (self-clearing): No	The alarm is raised when an SDP binding drops an MLD group because the configurable maximum number of MLD groups on the SDP binding is reached.
Name: SiteBgpAdVplsIdMisconfiguration (739) Type: configurationAlarm (11) Probable cause: bgpAdVplsIdInconsistent (439)	Severity: Major Object Type (class): BgpAdSite Domain: vpls Implicitly cleared (self-clearing): Yes	The alarm is raised when the configured VPLS ID on a BGP AD object differs from the VPLS ID configured for the VPLS site.
Name: SubscrAuthPolicyMisconfigured (271) Type: ConfigurationAlarm (15) Probable cause: SubscrAuthPolicyNotFound (203)	Severity: Warning Object Type (class): L2AccessItfDhcpRelayCfg Domain: vpls Implicitly cleared (self-clearing): Yes	The alarm is raised when a subscriber authentication policy for DHCP relay is misconfigured.
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm (18) Probable cause: networkDegradation (204)	Severity: Major Object Type (class): AbstractVpls Domain: vpls Implicitly cleared (self-clearing): Yes	The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.

(3 of 3)

Table 3-83 Domain: vprn

Alarm	Attributes	Description
Name: CommunityMisconfiguration (442) Type: serviceAlarm (16) Probable cause: CommunityMisconfiguration (347)	Severity: Major Object Type (class): Site Domain: vprn Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects a community misconfiguration on a service site.
Name: HashLabelMismatch (1113) Type: configurationAlarm (11) Probable cause: hashLabelMismatch (826)	Severity: Warning Object Type (class): Vprn Domain: vprn Implicitly cleared (self-clearing): Yes	The alarm is raised when the hash label is enabled on a VPRN site and disabled on another site in the service.
Name: InterfaceDown (36) Type: configurationAlarm (11) Probable cause: interfaceDown (32)	Severity: Major Object Type (class): IPMirrorInterface Domain: vprn Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects that an interface is operationally down.
Name: MaxNumExportRoutesReached (1116) Type: ProtocolAlarm (1) Probable cause: MaxNumExportRoutesReached (828)	Severity: Minor Object Type (class): Site Domain: vprn Implicitly cleared (self-clearing): Yes	The alarm is raised when the number of routes exported from a route table to a VRF reaches the configured maximum.
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm (18) Probable cause: networkDegradation (204)	Severity: Major Object Type (class): Vprn Domain: vprn Implicitly cleared (self-clearing): Yes	The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.

Table 3-84 Domain: vrrp

Alarm	Attributes	Description
Name: AdvNotActivated (741) Type: configurationAlarm (11) Probable cause: advertisementNotActivated (517)	Severity: Warning Object Type (class): InstanceV6 Domain: vrrp Implicitly cleared (self-clearing): Yes	The alarm is raised when the parent interface of an IPv6 VR instance is not configured to send router advertisements, or when router advertisement is not configured to use the virtual MAC address.
Name: AuthFailure (281) Type: authenticationAlarm (14) Probable cause: authFailure (46)	Severity: Major Object Type (class): AbstractInstance Domain: vrrp Implicitly cleared (self-clearing): No	The alarm is raised when authentication fails. The alarm information includes the source IP address.
Name: InstanceDown (284) Type: configurationAlarm (11) Probable cause: instanceDown (216)	Severity: Major Object Type (class): AbstractInstance Domain: vrrp Implicitly cleared (self-clearing): Yes	The alarm is raised when the 5620 SAM detects that a VRRP instance is operationally down.

(1 of 2)

Alarm	Attributes	Description
Name: IPListMismatch (282) Type: configurationAlarm (11) Probable cause: nonMatchingBackupAddressList (214)	Severity: Warning Object Type (class): AbstractInstance Domain: vrrp Implicitly cleared (self-clearing): Yes	The alarm is raised when the IP address list in an advertisement message from the current master does not match the configured IP address list.
Name: mismatchBackupAddress (279) Type: configurationAlarm (11) Probable cause: mismatchBackupAddress (212)	Severity: Minor Object Type (class): VRInstance Domain: vrrp Implicitly cleared (self-clearing): No	The alarm is raised when two VR instances in a VR have different backup addresses.
Name: mismatchSubnets (280) Type: configurationAlarm (11) Probable cause: mismatchSubnets (213)	Severity: Major Object Type (class): VRInstance Domain: vrrp Implicitly cleared (self-clearing): Yes	The alarm is raised when two VR Instances in a VR have backup addresses that are in different subnets.
Name: mismatchVrrpTypes (278) Type: configurationAlarm (11) Probable cause: mismatchVrrpTypes (211)	Severity: Minor Object Type (class): VRInstance Domain: vrrp Implicitly cleared (self-clearing): Yes	The alarm is raised when two VR instances in a VR are of different types, for example, when one VR instance type is Network and the other is IES.
Name: MultipleOwners (283) Type: configurationAlarm (11) Probable cause: multipleOwnersConfigured (215)	Severity: Major Object Type (class): AbstractInstance Domain: vrrp Implicitly cleared (self-clearing): No	The alarm is raised when an owner VR instance detects another instance that advertises itself as an owner.
Name: VirtualRouterDown (277) Type: configurationAlarm (11) Probable cause: virtualRouterDown (210)	Severity: Major Object Type (class): VrrpVirtualRouter Domain: vrrp Implicitly cleared (self-clearing): Yes	The alarm is raised when the aggregated Operational State of a VR is Down.

(2 of 2)

Table 3-85 Domain: vs

Alarm	Attributes	Description
Name: UndefinedSchedulerReference (118) Type: configurationAlarm (11) Probable cause: undefinedSchedulerReference (101)	Severity: Warning Object Type (class): ServiceTypeDefinition Domain: vs Implicitly cleared (self-clearing): Yes	The alarm is raised when a queue specified in the access ingress or access egress policy of an L2 access interface is not referenced by the scheduler policy for the interface.

4 — Troubleshooting services and connectivity

4.1 Troubleshooting services and connectivity

This chapter documents how to troubleshoot service and general connectivity problems when there is no associated alarm condition. See chapter 3 for information about troubleshooting a service using 5620 SAM alarms.

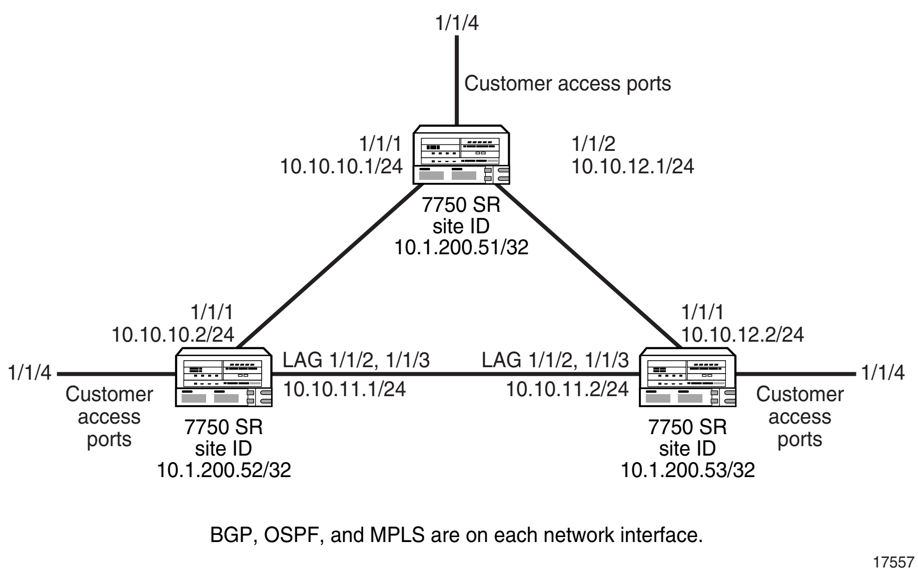
STM OAM diagnostics for troubleshooting

You can use the 5620 SAM Service Test Manager, or STM, OAM diagnostic tools to troubleshoot a service or transport. The STM provides the ability to group OAM diagnostic tests into test suites for more comprehensive fault monitoring and troubleshooting. A test suite can perform end-to-end testing of a customer service and the underlying network transport elements. The use of test suites is especially valuable when multiple objects of the same type require testing. Test suites can be scheduled to run on a regular basis to provide continual network performance feedback. See the *5620 SAM User Guide* for information about using the STM and creating scheduled tasks.

Sample network

Figure 4-1 shows a network that is used as an example for the OAM diagnostics procedures in this chapter.

Figure 4-1 Sample network



4.2 Workflow to troubleshoot a service or connectivity problem

Sequentially perform the following tasks until you identify the root cause of the problem.

1 Use the Manage→Services form to identify the service that you want to investigate.

2 Double-click on the service. The Service (Edit) form appears.

3 Verify that there are no alarms associated with the service by clicking on the Faults tab button in the Service form.

a If there are alarms that affect the service, see chapter 3.

b If there are no alarms that affect the service, go to step 4.

4 Determine whether the VPLS or VLL service is part of an H-VPLS configuration. See Procedure 4-1.

5 Verify whether the administrative and operational states of each component of the service are Up. See Procedure 4-2.

6 Verify the connectivity of the customer equipment using the entries in the FIB. See Procedure 4-3.

7 Verify that the 5620 SAM service configuration aligns with the customer requirements. For example, ensure that 5620 SAM configuration uses the correct service type and SAP configuration, and that the circuit and site are included in the service.

8 Verify the connectivity of all egress points in the service. See Procedure 4-4 or Procedure 4-5.

9 Use the results from the MAC Ping and MAC Trace diagnostics to choose one of the following options:

a If the MAC Ping, MEF MAC Ping, or MAC Trace diagnostics returned the expected results for the configuration of your network:

i Measure the frame transmission size on all objects associated with the service such as the service sites, access and network ports, service tunnels, and circuits. See Procedure 4-6.

ii Review the ACL filter policies to ensure that the ACL filter for the port is not excluding packets that you want to test. See Procedure 4-11.

iii Verify the QoS configuration.

b If the MAC Ping and MAC Trace diagnostics did not return the expected results for the configuration of your network:

i Verify the end-to-end connectivity on the service using the Service Site Ping diagnostic. See Procedure 4-7.

ii Verify the end-to-end connectivity on the service tunnel using the Tunnel Ping diagnostic. See Procedure 4-8.

iii Verify the end-to-end connectivity of an MPLS LSP using the LSP Ping diagnostic. See Procedure 4-9.

c If the MAC Ping diagnostic returned the expected results for the configuration of your network, and the MAC Trace diagnostic did not return the expected results for the configuration of your network:

i Verify that the correct service tunnels are used for the service.

ii Correct the service tunnel configuration, if required.

iii Review the route for the MPLS LSP using the LSP Trace OAM diagnostic. (For MPLS encapsulation, only.) If the LSP Trace results do not meet the requirements of your network, review the resource availability and configurations along the LSP expected routes. See Procedure 4-10.

10 Contact your Alcatel-Lucent technical support representative if the problem persists. See chapter 1 for more information.

4.3 Service and connectivity troubleshooting procedures

Use the following procedures to perform service and connectivity troubleshooting.

Procedure 4-1 To identify whether a VPLS is part of an H-VPLS

1. Choose Manage→Services from the 5620 SAM main menu.
2. Configure the list filter criteria, if required, and click on the Search button. A list of services appears at the bottom of the Manage Services form.
3. Choose the service associated with the service problem.
4. Click on the Properties button. The Service form opens.
5. Click on the Mesh SDP Bindings or Spoke SDP Bindings tab button.
6. Drag and drop the Service ID, VC ID, and Service Type columns to first three positions on the left side of the form.
7. Sort the list by VC ID.

If a VC ID has more than one unique Service ID, these services are involved in an H-VPLS relationship.

a If there are no alarms on the H-VPLS service, go to step 5 in General Procedure 4.2.

b If there are alarms on the H-VPLS service, see chapter 3 for more information.

Note — An alarm on a service can propagate across the services in the H-VPLS domain.

Procedure 4-2 To verify the operational and administrative states of service components

1 Click on the Components tab button on the *service* (Edit) form.

2 Open the tree, or right-click on the sites and choose Properties from the contextual menu. Review the states for the site using the Operational State and Administrative State parameters.

3 Click on the L2 Access Interfaces, L3 Access Interfaces, and Mesh SDP Bindings or Spoke SDP bindings tab buttons to review the operational and administrative states for the remaining components of the service.

4 Use the operation and administrative states of the service components to choose one of the following options:

a If the operational and administrative states for all service components are Up, go to step 6 in General Procedure 4.2.

b If the operational state is Down and the administrative state is Up for one or more service components, the 5620 SAM generates an alarm. You must investigate the root problem on the underlying object. See chapter 3 for more information.

c If the administrative state is Down for one or more service components, change the administrative state to Up. Go to step 6.

5 If the service problem persists, another type of service problem may be present. Perform the steps of the section 4.2 troubleshooting workflow.

6 If the workflow does not identify the problem with your service, contact your Alcatel-Lucent technical support representative. See section 1.4 for more information.

Procedure 4-3 To verify the FIB configuration

This procedure describes how to verify the connectivity of customer equipment on the service tunnel.

1 Click on the L2 Access Interfaces tab button on the Services (Edit) form. A list of L2 access interfaces appears.

2 Double-click on a row in the list. The L2 Access Interface form appears.

3 Click on the Forwarding Control tab button.

4 Click on the FIB Entries tab button.

5 Click on the Resync button.

- **a** If there is a list of FIB entries, confirm the number of entries with the customer configuration requirement. If the configuration meets the customer requirement, go to step 7 in General Procedure 4.2.

- **b** If there are no FIB entries, there is a configuration problem with the customer equipment or the connection from the equipment to the service tunnel.

  - **i** Confirm that the 5620 SAM service configuration aligns with the customer requirements.

  - **ii** Confirm that there are no problems with the customer equipment and associated configuration.

6 If the service problem persists, another type of service problem may be present. Perform the steps of the section 4.2 troubleshooting workflow.

7 If the workflow does not identify the problem with your service, contact your Alcatel-Lucent technical support representative. See section 1.4 for more information.

Procedure 4-4 To verify connectivity for all egress points in a service using MAC Ping and MAC Trace

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Manage Tests form appears.

2 Click on the Create button.

3 Choose L2 Service→Create MAC Ping from the Create contextual menu. The MAC Ping create form appears with the General tab button selected.

4 Clear the results from the previous diagnostic session from the Results tab, if necessary.

Note — You must use the MAC Ping and MAC Trace diagnostic to test the service in both directions for the connection.

5 Configure the parameters for the diagnostic session and run the diagnostic.

a 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. Enter the service ID for the VPLS or VLL service between the sites, and the sites you want to ping, in this case, from site ID 10.1.200.51/32 to site IDs 10.1.200.52/32 and 10.1.200.53/32 using the network in Figure 4-1.

Click on the Results tab to view the list of ping responses. Double-click on a row in the list to view its details.

b You can target the specific MAC address of a service site. Enter the target MAC address of the specific site in the service that you want to ping, in this case, from site ID 10.1.200.51/32 to site ID 10.1.200.52/32 using the network in Figure 4-1.

Click on the Results tab to view the list of ping responses. Double-click on a row in the list to view its details.

6 Review the results and assess whether the configuration meets the network requirements.

In particular, review the results in the Return Code column. Table 4-1 lists the displayed messages.

Table 4-1 MAC Ping OAM diagnostic results

Displayed message	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. The far-end egress point exists and is operating correctly. No action required.
fecNoMap (2)	The replying router has no mapping for the FEC.
notDownstream (3)	The replying router is not a downstream router.
downstream (4)	The replying router is a downstream router, and the mapping for this FEC on the router interface is the specified label.
downstreamNotLabel (5)	The replying router is a downstream router, and the mapping for this FEC on the router interface is not the specified label.
downstreamNotMac (6)	The replying router is a downstream router, but it does not have the specified MAC address.

(1 of 2)

Displayed message	Description
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.

(2 of 2)

7 Click on the Create button.

8 Choose L2 Service→Create MAC Trace from the Create contextual menu. The MAC Trace create form appears with the General tab button selected.

9 Configure the parameters for the diagnostic session and run the diagnostic. A MAC Trace shows the path, protocol, label, destination SAP, and hop count to the location of the destination MAC. Enter the service ID for the VPLS or VLL service between the sites, and the sites you want to trace, in this case, from site ID 10.1.200.51/32 to site IDs 10.1.200.52/32 and 10.1.200.53/32 using the network in Figure 4-1.

Click on the Results tab to view the list of trace responses. Double-click on a row in the list to view its details.

10 Review the diagnostic results and assess whether the configuration meets the network requirements.

a If MAC Ping and MAC Trace diagnostics returned the expected results for the configuration of your network, go to step 9 a in General Procedure 4.2.

b If MAC Ping and MAC Trace diagnostics did not return the expected results for the configuration of your network, go to step 9 b in general procedure 4.2.

c Go to step 9 c in General Procedure 4.2 if:

- MAC Ping diagnostic returned the expected result for the configuration of your network
- MAC Trace diagnostic did not return the expected result for the configuration of your network

Procedure 4-5 To verify connectivity for all egress points in a service using MEF MAC Ping

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Manage Tests form appears.

2 Click on the Create button.

3 Choose L2 Service→Create MEF MAC Ping from the Create contextual menu. The MEF MAC Ping create form appears with the General tab button selected.

4 Clear the results from the previous diagnostic session from the Results tab, if necessary.

Note — MEF MAC Ping must run simultaneously in both directions between the source and destination VPLS sites.

5 Configure the parameters for the diagnostic session and run the diagnostic.

You can target the specific MAC address of a service site. Enter the target MAC address of the specific site in the service that you want to ping.

Click on the Results tab to view the list of ping responses. Double-click on a row in the list to view its details.

6 Review the results and assess whether the configuration meets the network requirements.

In particular, review the results in the Return Code column. Table 4-2 lists the displayed messages.

Table 4-2 MEF MAC Ping OAM diagnostic results

Displayed message (return code)	Description
responseReceived (1)	A response was received on the device to the OAM diagnostic performed.
requestTimedOut (5)	The OAM diagnostic could not be completed because no reply was received within the allocated timeout period.

7 Review the diagnostic results and assess whether the configuration meets the network requirements.

- **a** If MEF MAC Ping diagnostics returned the expected results for the configuration of your network, go to step 9 a in General Procedure 4.2.

Procedure 4-6 To measure frame transmission size on a service using MTU Ping

1 Record the maximum frame transmission size for the service.

2 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form appears.

3 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.

4 Double-click on a service tunnel from the list. The Tunnel (Edit) form appears.

5 Click on the Tests tab button.

6 Click on the MTU Ping tab button.

7 Click on the Create button. The MTU Ping (Create) form appears with the General tab button selected. The form displays information about the service tunnel being tested and the originating tunnel ID.

Note — You must use the MTU Ping diagnostic to test the service in both directions for the connection.

8 Configure the parameters for the diagnostic session. Click on the Test Parameters tab button and enter the MTU value recorded in step 1 for the MTU End Size (octets) parameter.

9 Run the diagnostic. The MTU Ping increments the datagram size until it fails to pass through the SDP (service tunnel) data path, in this case, an MTU Ping from site ID 10.1.200.52/32 to site ID 10.1.200.53/32 using the network in Figure 4-1.

Click on the Results tab to view the list of trace responses. Double-click on a row in the list to view its details. The number of responses is determined by the incremental increase in datagram size.

10 Review the diagnostic results and assess whether the configuration meets the network requirements. Click on the Packets tab button.

a If the Status column displays Response Received for all circuits, the service tunnel supports the configured frame transmission size for the circuit. Go to step 9 a ii in General Procedure 4.2.

b If the Status column displays Request Timed Out for any of the circuits, the transmission failed at that frame size. If the frame size for the failure point is below the MTU value configured for the service, the packets are truncating along the service route. Investigate the cause of the truncated packets.

11 If the service problem persists, another type of service problem may be present. Perform the steps of the troubleshooting workflow in this chapter.

12 If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel-Lucent technical support representative. See section 1.4 for more information.

Procedure 4-7 To verify the end-to-end connectivity of a service using Service Site Ping

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Manage Tests form appears.

2 Click on the Create button.

3 Choose Service→Create Service Site Ping from the Create contextual menu. The Service site ping create form appears with the General tab button selected.

Note — You must use the Service Site Ping diagnostic to test the service in both directions for the connection.

4 Configure the parameters for the diagnostic session and run the diagnostic.

The originating service tunnel for the Service Site Ping is from site ID 10.1.200.51/32 to site ID 10.1.200.53/32, the other end of the service using the network in Figure 4-1.

Click on the Results tab to view the list of trace responses. Double-click on a row in the list to view its details.

5 Review the diagnostic results and assess whether the configuration meets the network requirements.

Table 4-3 lists the displayed messages.

Table 4-3 Service Site Ping OAM diagnostic 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 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 the responder.

a If the Service Site ping passes, the routes between the two sites are complete and in an operational state. If the MAC Ping performed in Procedure 4-4 failed:

i Investigate the status of the two SAPs used for the circuit.

ii Correct the configuration issue related to the SAPs, if required.

If there is no configuration problem with the SAPs, the service problem is related to the MAC addresses. The MAC address problem could be caused by the:

- ACL MAC filter excluding the required MAC address
- external customer equipment

b If the Service Site Ping fails, there is a loss of connectivity between the two sites.

i Log in to one of the sites using the CLI.

ii Enter the following command:

ping <*destination_site_ip_address*> ↵

where <*destination_site_ip_address*> is the address of the other site in the route

If the CLI IP ping passes, go to step 9 b ii of the section 4.2 troubleshooting workflow.

6 Use the CLI to verify that the IP address of the destination site is in the routing table for the originating site by entering:

show router route-table ↵

If the IP address for the destination site is not in the routing table for the originating site, there is an L3 or L2 problem.

i Verify that the appropriate protocols are enabled and operational on the two sites.

ii Verify the administrative and operational states of the underlying L2 equipment, for example, ports and cards.

7 If the service problem persists, another type of service problem may be present. Perform the steps of the section 4.2 troubleshooting workflow.

8 If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel-Lucent technical support representative. See section 1.4 for more information.

Procedure 4-8 To verify the end-to-end connectivity of a service tunnel using Tunnel Ping

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels 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 Tests tab button.

5 Click on the Tunnel Ping tab button.

6 Click on the Create button. The Tunnel Ping (Create) form appears with the General tab button displayed. The form displays information about the circuit being tested, including the originating tunnel ID.

Note — You must use the Tunnel Ping diagnostic to test the service in both directions for the connection.

7 Configure the parameters for the diagnostic session as follows.

- The Return Tunnel parameter must specify the return tunnel ID number, because the tunnels are unidirectional.
- From the Test Parameters tab button, the Forwarding Class parameter must specify the forwarding class for the service tunnel. Make sure that the forwarding classes for the service tunnels map to the QoS parameters configured for customer services, such as VLL.
- The Number of Test Probes and Probe Interval parameters must be configured to send multiple probes.

8 Run the diagnostic. Set the diagnostic configuration for a Tunnel Ping from site ID 10.1.200.51/32 to site ID 10.1.200.53/32 using the network in Figure 4-1, by specifying the return ID of the tunnel you want to test.

Click on the Results tab to view the list of trace responses. Double-click on a row in the list to view its details. Double-click on the entry in the Tunnel Ping results form to view the diagnostic details.

9 Review the diagnostic results and assess whether the configuration meets the network requirements.

Table 4-4 lists the displayed messages.

Table 4-4 Tunnel OAM diagnostic 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 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 was received, or before the timeout of the request occurred.
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.

a If the Tunnel Ping passes, the network objects below the tunnel are operating with no performance issues.

b If the Tunnel Ping fails, go to step 9 b iii of the section 4.2 troubleshooting workflow to verify the end-to-end connectivity of services using MPLS LSP paths, if required.

10 If the service problem persists, another type of service problem may be present. Perform the steps of the section 4.2 troubleshooting workflow.

11 If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel-Lucent technical support representative. See section 1.4 for more information.

Procedure 4-9 To verify end-to-end connectivity of an MPLS LSP using LSP Ping

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Manage Tests form appears.

2 Click on the Create button.

3 Choose MPLS→Create LSP Ping from the Create contextual menu. The LSP Ping (Create) form appears with the General tab button selected.

Note — You must use the LSP Ping diagnostic to test the service in both directions for the connection.

4 Configure the parameters for the diagnostic session and run the diagnostic. Target an LSP or an LSP path. Choose the MPLS site for the test, then configure the LSP you want to ping that is associated with the MPLS site, in this case, an LSP Ping from site ID 10.1.200.51/32 to site ID 10.1.200.52/32 using the network in Figure 4-1.

Click on the Results tab to view the list of trace responses. Double-click on a row in the list to view its details. Double-click on the entry in the LSP Ping results form to view the diagnostic details.

5 Review the diagnostic results and assess whether the configuration meets the network requirements.

Table 4-5 lists the displayed messages.

Table 4-5 LSP Ping OAM diagnostic results

Displayed message	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. The far-end egress point exists and is operating correctly. No action required.
fecNoMap (2)	The replying router has no mapping for the FEC.
notDownstream (3)	The replying router is not a downstream router.
downstream (4)	The replying router is a downstream router, and the mapping for this FEC on the router interface is the specified label.
downstreamNotLabel (5)	The replying router is a downstream router, and the mapping for this FEC on the router interface is not the specified label.
downstreamNotMac (6)	The replying router is a downstream router, but it does not have the specified MAC address.
downstreamNotMacFlood (7)	The replying router is a downstream router, but it does not have the specified MAC address and cannot flood the request to other routers.
malformedEchoRequest (8)	The received echo request is malformed.
tlvNotUnderstood (9)	One or more TLVs were not understood.

a If the LSP Ping passes, you have completed the workflow for troubleshooting services. Contact your Alcatel-Lucent technical support representative if the problem persists. See section 1.4 for more information.

b If the LSP Ping fails, verify the administrative and operational status of the underlying L2 equipment.

6 If the service problem persists, another type of service problem may be present. Perform the steps of the section 4.2 troubleshooting workflow.

7 If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel-Lucent technical support representative. See section 1.4 for more information.

Procedure 4-10 To review the route for an MPLS LSP using LSP Trace

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Manage Tests form appears.

2 Click on the Create button.

3 Choose MPLS→Create LSP Trace from the Create contextual menu. The LSP trace create form appears with the General tab button selected.

Note — You must use the LSP Trace diagnostic to test the service in both directions for the connection.

4 Configure the parameters for the diagnostic session and run the diagnostic. Target an LSP, any LSP or an LSP path. Choose the MPLS site for the test, then configure the LSP or LDP you want to trace that is associated with the MPLS site, in this case, an LSP Ping from site ID 10.1.200.51/32 to site ID 10.1.200.52/32 using the network in Figure 4-1.

Click on the Results tab to view the list of trace responses. Double-click on a row in the list to view its details. Double-click on the entry in the LSP Trace results form to view the diagnostic details.

5 Review the diagnostic results and assess whether the configuration meets the network requirements.

- **a** If the LSP Trace returned the expected results for the configuration of your network, the troubleshooting is complete.
- **b** If the LSP Trace did not return the expected results for the configuration of your network, verify that the correct MPLS LSP is used for the service.

6 If the service problem persists, another type of service problem may be present. Perform the steps of the section 4.2 troubleshooting workflow.

7 If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel-Lucent technical support representative. See section 1.4 for more information.

Procedure 4-11 To review ACL filter properties

1. Click on the L2 Access Interfaces or L3 Access Interfaces tabs on the Services (Edit) form. A list of interfaces appears.
2. Double-click on a row in the list. The L2 or L3 Interface configuration form appears.
3. Click on the ACL tab button.
4. Review the ingress and egress filter configurations to ensure that ACL filtering configurations do not interfere with the service traffic.
   a. If there are no ACL filtering configurations that interfere with the service traffic, go to step 9 a ii in General Procedure 4.2.
   b. If there are ACL filtering configurations that interfere with the service traffic, implement and verify the solution for the service problem.
5. If the service problem persists, another type of service problem may be present. Perform the steps of the section 4.2 troubleshooting workflow.
6. If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel-Lucent technical support representative. See section 1.4 for more information.

Procedure 4-12 To view anti-spoof filters

If a host is having a problem connecting to the network, one possibility for the problem is dropped packets as a result of anti-spoofing filters on the SAP. The 5620 SAM allows you to view the anti-spoof filters currently in effect on a SAP.

Anti-spoof filters are frequently created and deleted in the network. As a result, the 5620 SAM does not keep synchronized with the anti-spoof filters on the managed devices. However, the 5620 SAM allows you to retrieve, on demand, the current anti-spoof filters for a SAP.

1. Select Manage→Services from the 5620 SAM main menu. The Manage Services form opens.
2. Configure the list filter criteria and click on the Search button. A list of services appears at the bottom of the Manage Services form.
3. Select the service in the list for which you want to view the anti-spoof filters.
4. Click on the Properties button. The Service (Edit) form opens with the General tab displayed.
5. Click on the L2 Access Interfaces or L3 Access Interfaces tab button, depending on the service that you selected.
6. Select an interface from the list and click on the Properties button. The Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Anti-Spoofing tab button.

8 Click on the Filters tab button.

9 Click on the Search button to retrieve the current anti-spoof filters for the SAP. The Filters tab refreshes with a list of the current anti-spoof filters.

Procedure 4-13 To retrieve MIB information from a generic NE using the snmpDump utility

Perform this procedure to export all object values from the 5620 SAM-supported SNMP MIBs on a generic NE. The exported information may help with troubleshooting the generic NE configuration on the device or in the 5620 SAM.

1 Log in to a 5620 SAM main server station as one of the following users:

- Solaris—samadmin
- Windows—a local administrator

2 Open a console window.

3 Navigate to the appropriate directory in the following list:

- Solaris—*install_dir*/nms/bin
- Windows—*install_dir*\nms\bin

where *install_dir* is the server installation location, typically /opt/5620sam/server on Solaris and C:\5620sam\server on Windows

4 Perform one of the following:

a On a Solaris station, enter the following at the prompt:

`./snmpDump.bash` ***`option_list`*** ↵

b On a Windows station, enter the following at the prompt:

`snmpDump.bat` ***`option_list`*** ↵

where *option_list* is one or more of the options listed in Table 4-6

Note 1 — Each option must be separated by a space, as shown in the following example:

snmpDump.bash -v 3 -h 192.168.18.77 -u jsmith -apw mypass -ppw yoda

Note 2 — If an option has a default value, the default value is included in the option description.

Table 4-6 snmpDump options for Windows

Option	Description
-v *version*	The SNMP version in use on the generic NE, which can be 1, 2, or 3 Default: 2
-f *file_name*	The output filename Default: *host*-snmpDump.out in the current directory
-h *host*	The IP address or hostname of the generic NE Default: localhost
-c *community*	The SNMP community
-u *v3_user*	The SNMPv3 user name
-e *snmp_engine_ID*	The SNMP engine ID
-ap *v3_auth_protocol*	The SNMPv3 authorization protocol, which can be MD5 or SHA Default: MD5
-apw *v3_auth_password*	The SNMPv3 authorization password
-ppw *v3_privacy_password*	The SNMPv3 privacy password
-cn *v3_context_name*	The SNMPv3 context name
-ci *v3_context_ID*	The SNMPv3 context ID
-p *port*	The TCP port on the main server that snmpDump must use to reach the generic NE Default: 161
-t *timeout*	A communication timeout value
-r *retries*	The number of times to retry connecting to the generic NE

The utility displays status messages similar to the following as it initializes:

```
Init Products ...

Init ProductFamilyDefs ...

Init PollingDirectiveDefs ...

Start reading from Node ...
```

The utility then begins to retrieve the MIB tables. As It processes a MIB table, it lists the table name and the number of entries the table contains, as shown below:

```
IF-MIB.ifEntry : 21

IP-MIB.ipAddrEntry : 5

MPLS-LSR-STD-MIB.mplsInterfaceEntry : 8

MPLS-TE-STD-MIB.mplsTunnelEntry : 0

MPLS-TE-STD-MIB.mplsTunnelHopEntry : 0

MPLS-TE-STD-MIB.mplsTunnelARHopEntry : 0

MPLS-TE-STD-MIB.mplsTunnelCHopEntry : 0
```

```
MPLS-LDP-STD-MIB.mplsLdpEntityEntry : 3

MPLS-LDP-STD-MIB.mplsLdpEntityStatsEntry : 3

MPLS-LDP-STD-MIB.mplsLdpPeerEntry : 3
```

The utility is finished when the command prompt is displayed.

5 To view the utility output, open the file using a MIB browser or a text editor.

5 — Troubleshooting using topology maps

5.1 Network topology map overview

Several network topology maps are available on the 5620 SAM.

The maps display network objects. You can open contextual menus and submenus to open forms with additional information. For more information about topology maps, see the *5620 SAM User Guide*.

The maps can be used for provide a view of the network from different perspectives for monitoring and troubleshooting activities. Depending on your requirements, the maps can display a low-level equipment and interface network view, or a specific customer or service view. One or many maps can be open at the same time.

Table 5-1 lists the maps that are available and how they are accessed.

Table 5-1 5620 SAM map views

Menu option	Function
Application→Physical Topology	View the Physical Topology map.
Application→LSP Topology	View the LSP Topology map.
Application→Service Tunnel Topology	View the Service Tunnel Topology map.
Application→Flat Maps→Physical Topology	View the Physical Topology - Flat map.
Application→Flat Maps→LSP Topology	View the LSP Topology - Flat map.
Application→Flat Maps→Service Tunnel Topology	View the Service Tunnel Topology - Flat map.
Manage→Composite Services	Create composite services and view the Composite Service Topology map and the Composite Service Flat Topology map.
Manage→MPLS→MPLS Paths	Create MPLS paths and view topology map for provisioned MPLS paths. See the *5620 SAM User Guide* for more information about creating MPLS paths.
Manage→MPLS→Dynamic LSPs	Create LSPs and view topology for provisioned, actual, and CSPF LSP paths, and LSP cross-connects. See the *5620 SAM User Guide* for more information.
Manage→MPLS→Manual Bypass LSPs	
Manage→MLPS→Static LSPs	
Manage→Service Tunnels	Create service tunnels. See the *5620 SAM User Guide* for more information.
Create→Equipment→Create Group	Create topology groups to organize the network.
Create→Equipment→Create Physical Link	Create physical links to view L1 network connectivity.

The maps represent interfaces, paths, managed devices, and unmanaged devices, as described in Table 5-2.

Table 5-2 Map elements

Element type	Description
Device icon	Managed devices, such as a 7750 SR
Port icon	Managed access interface
Unmanaged device icon	Unmanaged device, such as a PE router
Topology group icon	Managed topology groups
Composite service icon	Managed composite services
Service tier icon	Services that make up the managed composite services
IP/MPLS cloud icon	IP/MPLS network
Green lines	Provisioned paths for an LSP map. Network interface that is operationally up for all other maps.
Gray lines	Actual paths for an LSP map
Red lines	Network interface that is operationally down

Interpreting map status indicators

The maps provide the following status information for managed network elements:

- operational status of a device
- operational status of an interface
- the most severe alarm for a device or service

Table 5-3 describes the map status indicators. There are no status indicators for unmanaged devices.

Table 5-3 Map status indicators

Indicator	Description
Device icon color	The color of device icons and links represents the reachability of the device. Red indicates that the device or link is not SNMP reachable. Yellow indicates that the device is being synchronized. Green indicates that the device is SNMP reachable. For a service view, red indicates that the service on the device is down.
Topology group icon	The color and icon in the upper left corner of the topology group icon indicate the most severe alarm on any of the devices in the group. The color of the upper middle section of the topology group icon indicates the aggregated SNMP connectivity status of the devices in the topology group. The color of the upper right corner of the topology group icon indicates the aggregated link status of the links in the topology group.

(1 of 2)

Indicator	Description
Composite service icon	The color and icon in the upper left corner of the composite service icon indicate the most severe alarm on any of the devices in the composite service. The color of the upper middle section of the composite service icon indicates the aggregated connectivity status of the devices in the composite service. The color of the upper right corner of the composite service icon indicates the aggregated link status of the links in the composite service.
Service tier icon	The color and icon in the upper left corner of the service tier icon indicate the most severe alarm on any of the devices belonging to the service. The color of the upper middle section of the service tier icon indicates the aggregated connectivity status of the devices belonging to the service. The color of the upper right corner of the service icon indicates the aggregated link status of the links belonging to the service.
Physical link	The color of physical links represents the status of the link. Gray indicates that the status of the link is unknown. Green indicates that the link is in service. Purple indicates that a physical link is being diagnosed. Red indicates that the link is out of service or failed.

(2 of 2)

Table 5-4 lists icon symbols and colors for 5620 SAM alarms.

Table 5-4 Map alarm status indicators

Map icon		Alarm	
Icon symbol	**Icon color**	**Severity**	**Color**
—	—	All	Grey
C	Red	Critical	Red
M	Orange	Major	Orange
m	Yellow	Minor	Yellow
W	Blue	Warning	Cyan
—	—	Condition	Mocha
—	—	Cleared	Green
—	—	Info	Light blue
—	White	No alarm	—

5.2 Troubleshooting alarms using topology maps

Use the following procedures to perform network monitoring and troubleshooting activities using the 5620 SAM maps.

Procedure 5-1 To monitor alarm status on maps

Use this procedure to view alarm information for network elements on a map.

1 Open one of the maps.

See Table 5-1 for information on how to access maps.

2 Resize or otherwise adjust the map window, as required, and arrange the icons for ease of management.

3 You can use the Zoom in Tool and Zoom out Tool buttons to adjust the map depending on the size of the network that you are viewing.

4 Monitor the map for any of the following conditions or changes:

- alarm status changes for an object
- loss of connectivity
- changes to the interface status of customer-facing equipment
- changes to the interface status of provider-facing equipment

5 Perform Procedure 5-2 to troubleshoot any problems that may arise.

Procedure 5-2 To find the source of an alarm using a map

Use this procedure to diagnose an alarmed network element using one of the maps.

1 Select the object with the alarm that you want to diagnose.

2 Right-click to view the contextual menu.

a When you right-click on an icon that represents a device or interface, choose Properties from the sub-menu for the selected object. The property form for the selected object opens.

b When you right-click on an interface:

i Choose List from the sub-menu. A form displays the interfaces for the selected path.

ii Choose an item from the list. One or more of the items may have an alarm condition, as indicated by color.

iii Click on the Properties button. The property form for the selected object opens.

3 Click on the Faults tab button. The Faults tab form opens.

4 View alarm status and diagnose the problem, as described in chapter 3.

Network management troubleshooting

6 — 5620 SAM LogViewer

6.1 5620 SAM LogViewer overview

The 5620 SAM LogViewer is a system monitoring and troubleshooting utility that parses, formats, and displays the contents of 5620 SAM log files. You can use LogViewer to do the following:

- View and filter real-time log updates.
- View, filter, and sort the entries in a static log view.
- Open compressed or uncompressed log files.
- Compare active logs in real time.
- Automatically send a notification when a specified type of entry is logged.

LogViewer is available on 5620 SAM main and auxiliary servers as a GUI and a CLI application. The GUI is more fully featured than the CLI, which is designed for use on a character-based console over a low-bandwidth connection, such as during a Telnet session.

LogViewer can interpret the various 5620 SAM log-file formats. The following restrictions apply to the files that LogViewer can open:

- The files must be local server or database logs.
- The files must be 5620 SAM Release 6.0 or later logs.

Configuration

The LogViewer GUI and CLI applications share a set of configuration options; changes made to these options by one application affect the other. Other options apply to the GUI only. You can customize LogViewer by creating and saving log filters and log profiles that are available to all GUI and CLI users, and can save the GUI application configuration, or workspace, to have LogViewer display the currently open logs the next time it starts. LogViewer does not save the current filter and display configuration for a log when you close the log unless you export the configuration to a log profile.

Filters

You can use the LogViewer CLI or GUI to create multiple filters that define the log entries that are displayed in a log view. A filter uses Java regular expressions as match criteria to specify which entries to display and optionally uses colors to identify the filtered entries.

Plug-ins

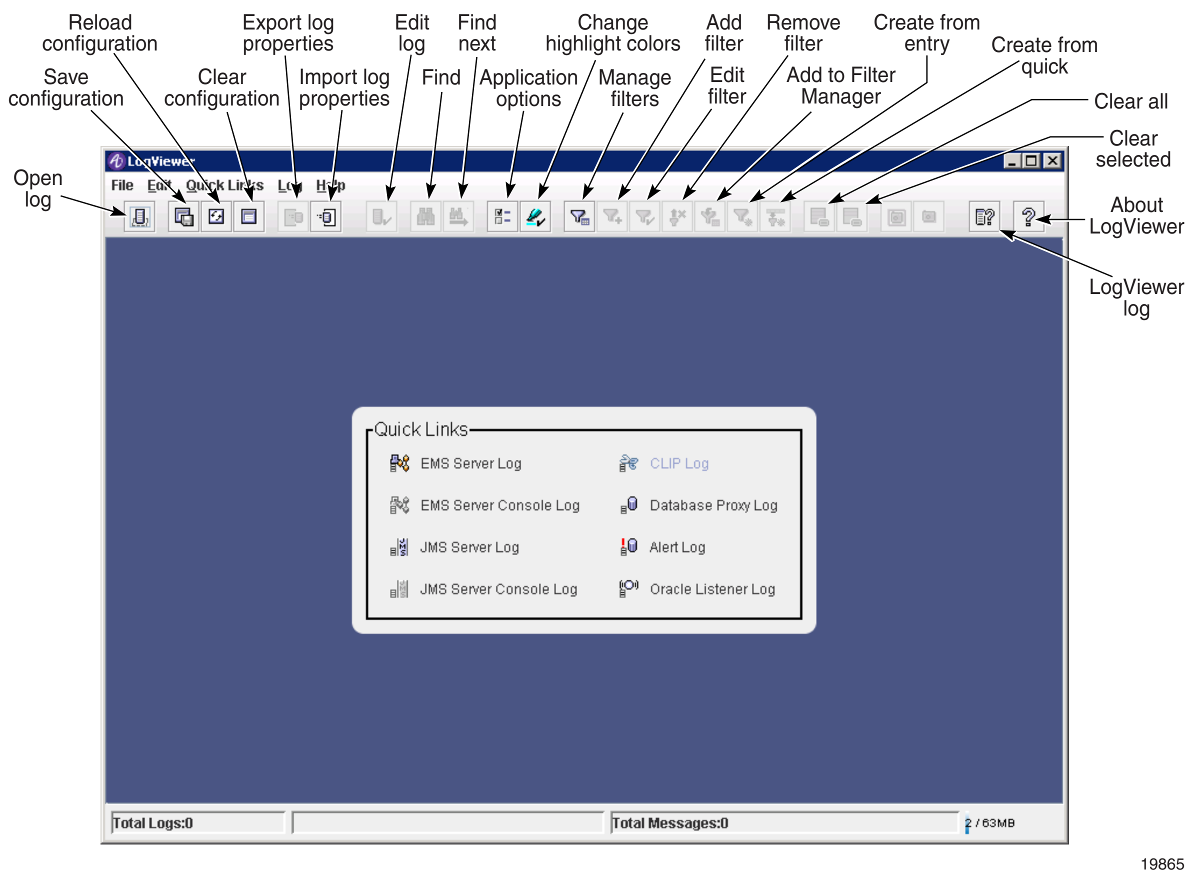
LogViewer supports the use of plug-ins to provide additional functionality. You can specify a plug-in for use with a specific log, or assign a default plug-in configuration that applies to the subsequently opened logs.

LogViewer has default plug-ins that can send notifications, such as e-mail messages and GUI pop-ups, when a new log entry matches a set of filter criteria. The LogViewer e-mail plug-in uses SMTP as the transport.

6.2 LogViewer GUI

The LogViewer GUI opens to display a Quick Links panel that has shortcuts to the logs that are present on the local file system. When you click on a log shortcut, LogViewer opens a tab that displays the most recent log entries. Figure 6-1 shows the LogViewer GUI with the Quick Links panel displayed and describes the main tool bar buttons.

Figure 6-1 LogViewer GUI showing Quick Links panel

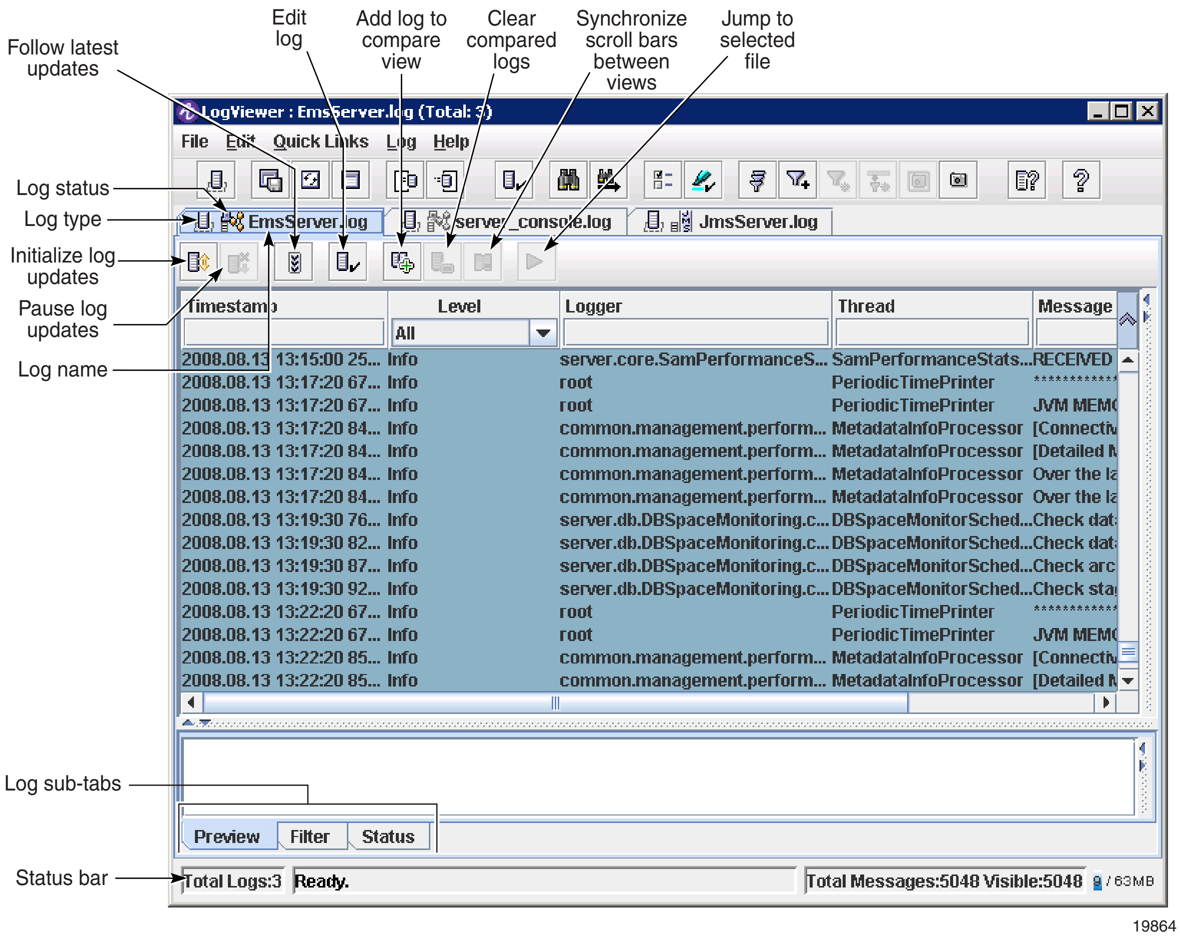


Overview

Each log that you open using the LogViewer GUI is displayed on a separate tab whose label contains the name of the log profile and an icon that indicates the log type. The log entries are highlighted using the colors configured for the log debug levels. A log tab that displays dynamic log updates also has a tool bar for common operations.

Figure 6-2 shows the LogViewer GUI with multiple open logs and describes the tool bar buttons on a tab that displays a currently active log.

Figure 6-2 LogViewer GUI showing log tabs



The lower panel of a log tab contains the following sub-tabs:

- Preview—displays the unparsed log-file text for the currently selected log entries
- Filter—lists and permits management of the currently active filters for the log
- Status—displays status information about the current log
- Plugin—displays information about the plug-ins associated with the log
- Legend—displays a legend that correlates log file names to the numbers in the File column on a log tab that contains multiple open logs, for example, merged logs; is not shown for log comparisons

The LogViewer GUI allows you to drag and drop a log file from another application into the GUI window. If you drop a file onto an open log tab, LogViewer provides options such as merging or comparing the log with another.

You can open a tab to list static log entries, such as the contents of an archived log or a snapshot of entries from an active log, and can pause the updates to active logs. The GUI also includes a text-search function.

GUI-based log filtering

The GUI provides a Filter Manager applet that lists the filters defined using the CLI or GUI and allows filter creation, modification, and deletion. A GUI operator can also use Filter Manager to test the regular expressions as filter match criteria.

To rapidly isolate a specific log entry or type of entry, you can create a temporary filter, or quick filter, by entering a regular expression in the field below a column header on a log tab. You can convert a quick filter to a saved filter for later use. A drop-down menu above the Level column allows the immediate filtering of log entries based on the debug level

A color that is specified as the highlight color for a filter is saved with the filter and applies to all logs that use the filter.

6.3 LogViewer CLI

The CLI-based 5620 SAM LogViewer works like the UNIX tail command when in display mode. The command mode has a multiple-level menu that you can display at any time. You can specify a command or log file using the minimum number of unique characters in the name, and can quickly toggle between the command and display modes. LogViewer buffers new log entries while in command mode and displays them when it returns to display mode.

The LogViewer CLI assigns a different color to each logging level, for example, WARN or INFO, using standard ANSI color attributes that can be specified as CLI startup options or configured through the GUI. The CLI also supports the use of filters, plugins, and quick links.

6.4 LogViewer GUI procedures

The following procedures describe how to use the LogViewer GUI application.

Procedure 6-1 To display logs using the LogViewer GUI

Perform this procedure to start the LogViewer GUI application and view one or more logs. See Figures 6-1 and 6-2, or move the mouse cursor over a GUI object, to view a description of the object, for example, a tool bar button.

1 Log in to the 5620 SAM server as an administrator.

Note — If the 5620 SAM server is installed on Solaris, you must log in as the samadmin user.

2 Perform one of the following.

a If the 5620 SAM server is installed on Solaris, run the following script:

path/nms/bin/logviewerui.bash

where *path* is the 5620 SAM server installation location, typically /opt/5620sam/server

b If the 5620 SAM server is installed on Windows, run the following script:

path\nms\bin\logviewerui.bat

where *path* is the 5620 SAM server installation location, typically C:\5620sam\server

The LogViewer GUI opens with the Quick Links panel or the log tabs in the saved workspace displayed.

3 To open a log file, perform one of the following:

a If the Quick Links panel is displayed, click on a link to view the associated log file.

b Choose Quick Links→*log_name* from the LogViewer main menu.

c To open a recently viewed log, choose File→Recent Logs→*log_file_name* from the LogViewer main menu.

d To browse for a log file, perform the following steps:

i Choose File→Local Log File from the LogViewer main menu or click on the Open log button in the main tool bar. The Local Log File form opens.

ii Use the form to navigate to the log-file location.

iii Select a log file and click on the Add button between the form panels. The log is listed in the panel on the right.

Note — The log file can be in compressed or uncompressed format.

iv If LogViewer cannot determine the type of log that the file contains, for example, if a log file is renamed, it sets the Type to Other. Use the Type drop-down menu to specify the log type, if required.

v Configure the Max. Messages parameter to specify the maximum number of entries that are listed on the log tab. LogViewer removes the oldest entries as required to keep the number of entries at or below this value.

vi Configure the Auto-Tail parameter to specify whether the log tab dynamically displays the log updates.

vii Click on the OK button. The Local Log File form closes.

e Drag and drop a log file into a section of the LogViewer main window that does not contain a log tab.

f Drag and drop a log file onto a log tab in the LogViewer main window. The Add File form opens. Perform the following steps:

i Choose one of the following options:

- New View—specifies that the log is displayed on a new log tab
- Replace Existing File—specifies that the log tab displays the new log instead of the current log
- Add to View—specifies that the entries in the new log and the entries in the current log are merged into one list on the same log tab
- Add to Compare View—specifies that the new log is to be displayed on the same log tab as the current log in a separate panel for comparison

ii Click on the OK button. The new log is displayed as specified.

A log tab opens to display the most recent entries in a log. If the log is active and the Auto-Tail parameter is enabled, the list scrolls upward to display new log entries as they are generated.

Note — The Auto-Tail parameter for a log is enabled by default.

Common display operations

4 To specify which columns are displayed on a log tab, right-click on a column header, and select or deselect the column names in the contextual menu, as required.

5 To reposition a column, drag the column title bar to the desired position, or right-click on the column header and choose Move Left or Move Right from the contextual menu.

6 To view the raw log-file text of one or more entries, select the entries. The entry text is displayed on the Preview sub-tab.

7 To restrict the list of displayed entries to a specific debug level, choose a debug level from the drop-down list under the Level column header.

8 To find log entries that contain a specific text string, perform the following steps.

i Choose Edit→Find from the LogViewer main menu. The Find form opens.

ii Specify a text string to search for using the text field and search options on the form.

Note — The LogViewer Find function does not support the use of regular expressions.

iii Click on the Find button, as required, to find the next list entry that contains the text string.

iv To find all list entries that contain the text string, click on the Find All button. The Find form closes and a new log tab opens to display the result of the search.

v Close the Find form if it is open.

Note — After you close the Find form, you can use the F3 key or the Find next button on the main tool bar to perform repeated find operations for the same text string on the same log tab.

9 To remove one or more log entries from the current view, perform one of the following.

a To clear all listed log entries, choose Log→Clear All Events from the LogViewer main menu, or click on the Clear all button in the main tool bar.

b To clear the currently selected log entries, choose Log→Clear Selected Events from the LogViewer main menu, or click on the Clear selected button in the main tool bar.

10 To apply a quick filter, enter a regular expression as a match criterion in the field below a column header and press ↵. The list is cleared, and only subsequent log entries that match the criterion are displayed. See Procedure 6-3 for more information about using filters.

11 Repeat 10 step to apply an additional quick filter, if required.

12 To apply a saved filter, perform the following steps.

i Choose Log→Add Filter from the LogViewer main menu, or click on the Add filter button in the main tool bar. The Select Filters form opens.

ii Select one or more filters in the list and click on the OK button. The filters are applied to the log view and are listed on the Filters sub-tab of the log tab.

See Procedure 6-3 for information about creating saved filters.

13 To remove a filter from the log, select the filter in the Filter sub-tab and choose Log→Remove Selected Filters, or click on the Remove filter button in the main tool bar.

14 If the log display is static, such as for an archived log or the result of a Find All operation, go to step 21.

Dynamic view operations

15 To edit the log display properties, choose Edit→Edit Log from the LogViewer main menu, or click on the Edit log button in the log tab tool bar, and perform the following steps.

i Configure the Max. Messages parameter to specify the maximum number of entries that are listed on the log tab. LogViewer removes the oldest entries as required to keep the number of entries at or below this value.

ii Configure the Auto-Tail parameter to specify whether the log tab dynamically displays the log updates.

iii Click on the OK button to close the Local Log File form.

16 To pause the display of log-file updates, choose Log→Pause from the LogViewer main menu, or click on the Pause log updates button in the log tab tool bar.

17 To resume the display of log-file updates, choose Log→Initialize Connection from the LogViewer main menu, or click on the Initialize log updates button in the log tab tool bar.

18 By default, a dynamic log view focuses on a new log entry. To focus the display on an earlier log entry and prevent the display from automatically focusing on a new log update, click on the Follow latest updates button in the log tab tool bar. Click on the button again to enable the default behavior.

19 To compare logs in real time, perform the following steps.

i Choose Log→Specify Compare from the LogViewer main menu, or click on the Add log to compare button on the log tab tool bar. The Compare Files form opens.

ii Use the form to navigate to the log-file location.

iii Select a log file and click on the Add button between the form panels. The log is listed in the panel on the right.

Note — The log file can be in compressed or uncompressed format.

iv If LogViewer cannot determine the type of log that the file contains, for example, if a log file is renamed, it sets the Type to Other. Use the Type drop-down menu to specify the log type, if required.

v Click on the OK button. The Compare Files form closes, and a second panel opens on the log tab to display the specified log.

The log entry lines are synchronized by timestamp. Dynamic log updates to each log are displayed as they occur. Blank entry lines serve as spacers to preserve the chronological order of the combined log entries.

vi By default, the scroll bars in the two panels are synchronized; when you scroll in the right panel, the display in the left panel scrolls by the same amount. Click on the Synchronize scroll bars between views button in the log tab tool bar to disable or re-enable this behavior, as required.

vii To remove the added log from the comparison, choose Log→Clear Compare from the LogViewer main menu, or click on the Clear compared logs button on the log tab tool bar. The right panel is removed from the log tab form.

20 To capture one or more log entries for display in a static view on a separate tab, perform one of the following.

a To capture all listed log entries, choose Log→Full Snapshot from the LogViewer main menu, or click on the Snap all button in the main tool bar.

b To capture the currently selected log entries, choose Log→Snapshot from the LogViewer main menu, or click on the Snap selected button in the main tool bar.

A new tab opens to display the captured log entries in a static view.

Static view operations

21 To sort a list of log entries in a static view, right-click on a column header and choose Sort Ascending, Sort Descending, or No Sort from the contextual menu. The log entries are sorted accordingly.

Note — You cannot sort the log entries in a dynamic view, but you can sort the entries in a snapshot of a dynamic log view.

22 To save the current workspace for subsequent sessions, choose File→Save Workspace from the LogViewer main menu, or click on the Save configuration button in the main tool bar.

23 Choose File→Exit from the LogViewer main menu to close the LogViewer GUI.

Procedure 6-2 To configure the LogViewer application using the GUI

Perform this procedure to use the LogViewer GUI to configure general application options for the LogViewer GUI and CLI applications.

1 Open the LogViewer GUI.

2 Choose Edit→Options→General from the LogViewer main menu, or click on the Application options button in the main tool bar. The Options form opens with the General tab displayed.

3 Configure the parameters:

- Last Directory—Click in the parameter field and use the browser form that opens to specify where to save exported log profiles.
- Base File Messages Directory—Click in the parameter field and use the browser form that opens to specify the base 5620 SAM log directory.
- Default Log Pattern—Edit this parameter to specify a regular expression that LogViewer uses to interpret log-file contents.
- Show Memory Monitor—Select this parameter to display the memory monitor at the bottom right corner of the LogViewer window.
- Quick Links Refresh Time (ms)—Enter a value to specify how often LogViewer refreshes the Quick Links list.
- Regular Expression Help URL—Enter a value to specify the location of the Java regular-expression help web page that opens when you click on the Help button while testing a regular expression for a filter.
- Web Browser Location—Enter a value to specify the location of the local file browser used to open the Java regular-expression help web page.
- Hide Table Tooltips—Select this parameter to suppress the display of tool tips when the mouse pointer moves over log entries in a log tab.
- Advanced Quick Filter—Select this parameter to display the advanced Quick Filter table header on log tabs.
- Display Advanced Quick Filter—Select this parameter to display the advanced Quick Filter table header on the log tab when a log file is opened.
- Rollover Remove Size—Enter a value to specify the number of log entries to remove from the LogViewer display when the maximum number of displayed log entries is reached.
- Delay for local file polling (ms)—Enter a value to specify, in ms, how long LogViewer waits before it checks local log files for updates.
- Default Date Format—Enter a colon-separated string to specify the LogViewer date format using y for year digits, M for month digits, d for date digits, H for hour digits, m for minute digits, s for second digits, and S for millisecond digits, for example, yyyy:MM:dd HH:mm:ss:SSS.
- Memory Monitor Threshold (%)—Enter a value to specify the percentage of available memory that LogViewer uses before it stops displaying log updates.
- Max. Recent Files—Enter a value to specify the number of files that LogViewer keeps in the list of recently opened files.
- LogViewer Log Level—Choose a logging level from the drop-down list to specify the minimum log level of the LogViewer application messages.
- Enable Viewer Performance Stats—Select this parameter to enable the display of LogViewer performance statistics.
- Stats Timer (seconds)—Enter a value to specify the number of seconds that LogViewer waits between log statistics updates.

4 Click on the Command Line tab button to configure the LogViewer CLI application.

5 Configure the following parameter:

- Command line buffer size—Enter a value to specify the number of log messages that LogViewer buffers when the CLI application is in command mode.

6 Choose an ANSI display attribute from the drop-down list beside each of the following parameters to specify how the CLI application displays the corresponding text.

- Normal Display—for normal application text
- Trace Level Display—for trace-level log entries
- Debug Level Display—for debug-level log entries
- Info Level Display—for info-level log entries
- Warning Level Display—for warning-level log entries
- Error Level Display—for error-level log entries
- Fatal Level Display—for fatal-level log entries
- Filter Display—for filtered log entries

7 Click on the SAM tab to configure the parameters that are specific to the 5620 SAM.

8 Configure the following parameters by clicking in the parameter field and using the browser form that opens to specify a directory:

- Database Location—specifies the base 5620 SAM database installation directory
- Oracle Location—specifies the base 5620 SAM Oracle installation directory
- NMS Root—specifies the nms directory under the base 5620 SAM server installation directory

9 Click on the Advanced tab to configure the parameters related to LogViewer performance.

Caution — The parameters on the Advanced tab typically require configuration only when LogViewer has performance problems. Consult Alcatel-Lucent technical support before you attempt to modify a parameter on the Advanced tab, as it may affect server performance.

Procedure 6-3 To manage filters using the GUI Filter Manager

Perform this procedure to create, modify, assign or delete a LogViewer filter.

Note — The Filter Manager is opened from within LogViewer, but runs as a separate applet. This enables the dragging and dropping of filters between Filter Manager and the Filters sub-tab of a lob tab.

1 Choose Log→Filter Manager from the LogViewer main menu. The Filter Manager applet opens.

2 Perform the following steps to add a filter.

i Click on the Add button. The Add Filter form opens.

ii Configure the Name parameter by specifying a unique name for the filter.

iii Configure the following parameter that correspond to the fields in a log entry by entering a regular expression as a filter criterion for each:

- Level
- Thread
- Message
- Logger
- Timestamp

iv Test a regular expression that you enter by clicking on the Test button beside the regular expression. The Regular Expression form opens.

v Paste an example log entry that you want to match using the regular expression into the Example field.

vi Click on the green right-pointing arrow to test the expression. If the expression is invalid, a message is displayed to indicate the error in the expression.

vii Correct the errors in the expression.

viii Repeat steps 2 vi and 2 vii until no error message is displayed.

ix Repeat steps 2 iv to 2 viii to test additional regular expressions, if required.

x Enable the Color parameter and click in the field beside the parameter to specify a highlight color for the matching log entries. A standard color chooser form opens.

xi Use the form to specify a color and click on the OK button. The color chooser form closes and the Add Filter form reappears.

xii Click on the OK button. The Add Filter form closes and the Filter Manager form lists the new filter.

3 To create a saved filter based on the current quick filter, perform the following steps.

i Choose Log→Create from Quick Filter from the LogViewer main menu, or click on the Create from quick button in the main tool bar. The Add Filter form opens and is populated with the quick filter match criteria.

ii Modify the match criteria as required.

iii Click on the OK button to save the filter.

4 To create a saved filter using a log entry as a template, perform the following steps.

i Select a log entry.

ii Choose Log→Create from Selected from the LogViewer main menu, or click on the Create from entry button in the main tool bar. The Add Filter form opens and is populated with the current log-entry field values as match criteria.

iii Modify the match criteria as required.

iv Click on the OK button to save the filter.

5 To make a copy of a filter, select the filter and click on the Copy button. A copy of the filter is listed on the Filter Manager form.

6 To edit a filter, select the filter and click on the Edit button. Configure the parameters described in step 2.

7 To delete a filter, select the filter and click on the Delete button

Procedure 6-4 To specify a plug-in using the LogViewer GUI

Perform this procedure to configure and enable plug-ins for a log file.

1 Choose File→Local Log File from the LogViewer main menu, or click on the Open log button in the log tab tool bar. The Local Log File form opens.

2 Use the form to navigate to the log-file location.

3 Select a log file and click on the Add button between the form panels. The log is listed in the panel on the right.

Note — The log file can be in compressed or uncompressed format.

4 Click on the Plugins tab button.

5 Choose a plug-in from the Plugin drop-down list.

6 If you choose the Bring to Front plug-in, perform the following steps.

i Specify a regular expression as a match criterion in the Message Filter field.

ii Go to step 8.

7 If you choose the E-Mail plug-in, perform the following steps.

i Specify a regular expression as a match criterion in the Message Filter field.

ii Configure the parameters:

- To—specifies the e-mail address of the recipient
- Password—specifies an SMTP password
- Message Filter—specifies a regular expression that is used as a filter to identify the log entries that invoke the plug-in
- Minimum E-mail Time (minutes)—specifies the minimum time between messages that the plug-in sends, to prevent e-mail flooding
- User—specifies a user name associated with the plug-in
- Host—specifies the name of an SMTP e-mail server
- Body Prefix—specifies the text that precedes the log-entry text in an e-mail message
- From—specifies the sender e-mail address used by the plug-in
- Subject—specifies the e-mail message subject line

8 Click on the OK button. The Local Log File form closes.

6.5 LogViewer CLI procedures

The following procedures describe how to use the LogViewer CLI application.

Procedure 6-5 To display logs using the LogViewer CLI

Perform this procedure to start the LogViewer CLI application and view one or more logs.

1 Log in to the 5620 SAM server as an administrator.

Note — If the 5620 SAM server is installed on Solaris, you must log in as the samadmin user.

2 Perform one of the following.

a If the 5620 SAM server is installed on a Solaris workstation, run the following script:

```
# path/nms/bin/logviewer.bash argument options parameter ↵
```

where
path is the 5620 SAM server installation location, typically /opt/5620sam/server
argument is an argument listed in Table 6-1
options is one or more of the options listed in Table 6-2
parameter is a parameter listed in Table 6-3

b If the 5620 SAM server is installed on a Windows PC, run the following script:

```
path\nms\bin\logviewer.bat argument options parameter ↵
```

where
path is the 5620 SAM server installation location, typically C:\5620sam\server
argument is an argument listed in Table 6-1
options is one or more of the options listed in Table 6-2
parameter is a parameter listed in Table 6-3

Table 6-1 LogViewer CLI startup arguments

Argument	Meaning
--version	Display LogViewer version information.
--help	Display LogViewer CLI help text.

Table 6-2 LogViewer CLI startup options

Option	Meaning
-counter	Prepend a counter number to each displayed log entry.
-parseAll	Parses and display the entire contents of a file before displaying the real-time updates.
-ansi *level attribute*	Display events and filters using ANSI-specified colors where *level* is a logging level, such as debug *attribute* is an ANSI color attribute, such as 42m to specify the color green
-quit	Quit LogViewer after parsing the log files.

Table 6-3 LogViewer CLI startup parameters

Parameter	Meaning
-xml *file_name*	Read information such as log file, plug-in and filter specifications from the XML file specified by *file_name*. The LogViewer GUI can export this information to an XML file.
file name	Display the specified file when LogViewer starts.

The LogViewer CLI opens in display mode. If a log file is specified as a startup parameter, the most recent entries in the log file are displayed as they are written to the log file. Otherwise, a cursor is displayed.

3 Enter command mode by pressing ↵. The following prompt is displayed:

```
log>
```

This prompt is called the root prompt. Table 6-4 describes the options that are available at the root prompt.

Table 6-4 LogViewer CLI root menu options

Option	Function
open	opens a submenu for choosing the logs to view
include	opens a submenu for specifying which log files to list in the *open* submenu
filter	opens a submenu for adding, listing or deleting filters
plugin	opens a submenu for adding, listing or delete plugins
options	opens a submenu for configuring LogViewer CLI and GUI application options
list	lists the files in the *open* submenu file list
reset	resets the log message counts
stats	displays LogViewer statistics for the current log
The following options are also available in submenus:	
back	goes to the previous menu
root	goes to the root menu
quit	quits the application
return	returns to display mode

4 Enter the following at the prompt:

open ↵

The following prompt is displayed:

```
log-open>
```

5 Press ↵ to display the list of available logs.

6 Perform one of the following.

a To view a log in the list, enter the name of a log at the prompt and press ↵.

b To view a log that is not listed, perform the following steps.

i Enter the following at the prompt:

other ↵

The following prompt is displayed:

`File Name (full path)?`

ii Enter the absolute or relative path of the log file that you want to open and press ↵. LogViewer opens the file.

7 Enter the following at the prompt to enter display mode and view the real-time log updates:

`return` ↵

LogViewer enters display mode. Log updates are displayed as they occur.

8 To add a filter that restricts the types of log entries that are displayed during the current LogViewer session, perform the following steps.

i Press ↵ to enter command mode.

ii Enter the following at the prompt to return to the root menu:

`root` ↵

The following prompt is displayed:

`log>`

iii Enter the following at the prompt:

`filter` ↵

The following prompt is displayed:

`log-filter>`

Note — You can also use commands at this menu level to list and delete filters.

iv Enter the following at the prompt:

`add` ↵

The following prompt is displayed:

`Filter name:`

v Enter a name for the filter and press ↵.

vi The following prompts are displayed in sequence:

`Level:`

`Logger:`

`Thread:`

`Timestamp:`

`Message:`

At each prompt, enter a regular expression to use as a match criterion, if required, and press ↵.

vii The following prompt is displayed:

```
Display Filter? (Y/N):
```

Enter y ↵ to apply the filter to the current log display. LogViewer applies the filter.

viii Enter the following to return to display mode:

return ↵

LogViewer enters display mode. The log updates are filtered before they are displayed.

9 To list the available log files, perform the following steps.

i Press ↵ to enter command mode.

ii Enter the following at the prompt:

list ↵

LogViewer lists the available log files.

iii Enter the following at the prompt to return to display mode:

return ↵

10 To display statistics about the current LogViewer session, perform the following steps.

i Press ↵ to enter command mode.

ii Enter the following at the prompt:

stats ↵

LogViewer displays statistics about the current session.

iii Enter the following at the prompt to return to display mode:

return ↵

11 To reset the statistics counters for the current LogViewer session, perform the following steps.

i Press ↵ to enter command mode.

ii Enter the following at the prompt:

reset ↵

LogViewer resets the counters.

iii Enter the following at the prompt to return to display mode:

`return` ↵

12 Enter the following at the prompt to close LogViewer:

`quit` ↵

Procedure 6-6 To configure the LogViewer CLI

Perform this procedure to use the LogViewer CLI to configure general CLI application options.

Note — The options configured in this procedure apply only to the current LogViewer CLI session.

1 Open the LogViewer CLI.

2 To add a file to the list of files in the *open* menu, perform the following steps.

i Press ↵ to enter command mode.

ii Enter the following at the root prompt:

`include` ↵

The following prompt is displayed:

`log-include>`

iii Enter the following at the prompt:

`add` ↵

The following prompt is displayed:

`File Name (full path)?`

iv Enter the absolute or relative path of the log file that you want to add and press ↵. LogViewer adds the file to the list in the *open* menu.

Note — The LogViewer CLI supports file drag-and-drop functionality.

v Enter the following at the prompt to return to the root prompt:

`root` ↵

3 To configure LogViewer file parsing, perform the following steps.

i Press ↵ to enter command mode.

ii Enter the following at the root prompt:

`options` ↵

The following prompt is displayed:

`log-options>`

iii Enter y ↵ at the prompt to confirm the action.

iv To specify whether LogViewer parses the entire log file, enter the following at the prompt:

`parseAll` ↵

A confirmation prompt is displayed.

v To force LogViewer to reparse the current log file, enter the following at the prompt:

`reparse` ↵

vi If you are prompted to enable parsing of the entire log file, enter y ↵.

vii Enter the following at the prompt to return to the root prompt:

`root` ↵

Procedure 6-7 To specify plug-ins using the CLI

Perform this procedure to specify a plug-in for the current LogViewer CLI session.

1 Open the LogViewer CLI.

2 Press ↵ to enter command mode.

3 Enter the following at the root prompt:

`plugin` ↵

The following prompt is displayed:

```
log-plugin>
```

4 Enter the following at the prompt:

add ↵

LogViewer displays a list of the available plug-ins and the following prompt:

```
Which plugin would you like to specify? (name)
```

5 Enter the name of a plug-in from the list and press ↵.

6 You may be prompted for plug-in configuration information. Supply the information, as required.

Note — The currently available plug-ins and the associated configuration options are described in Procedure 6-4.

7 — Troubleshooting network management LAN issues

7.1 Troubleshooting network management domain LAN issues

The following procedures describe how to troubleshoot network management domain LAN issues.

Procedure 7-1 Problem: All network management domain PCs and workstations are experiencing performance degradation

1 Verify that there is sufficient bandwidth between the elements of the network management domain.

Bandwidth requirements vary depending on the type of management links set up, and the number of devices in the managed networks. For information about network planning expertise, contact your Alcatel-Lucent technical support representative.

See the *5620 SAM Planning Guide* for more information about the bandwidth requirements.

2 When you are using in-band management, ensure that the network devices used to transport the management traffic are up. Ping each of the devices to ensure the management traffic can flow along the in-band path.

In-band management 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 virtual interfaces.

Procedure 7-2 Problem: Lost connectivity to one or more network management domain PCs or workstations

If you can ping a PC or workstation, but are still unable to connect to a machine to perform a function, there may be a problem with a specific application.

You can also use Procedure 7-3 to check the following:

- ports that need to be open across firewalls
- routing using netstat and ARP

1 Open a command console or DOS shell on the PC or workstation.

2 Try to ping the host name of the workstation or PC by typing:

a For PCs:

ping name_of_machine ↵

where *name_of_machine* is the name of the network management domain PC

b For workstations:

ping -s *name_of_machine* ↵

where *name_of_machine* is the name of the network management domain workstation

3 Review the output. The following shows sample output.

```
# ping -s name_of_machine

PING name_of_machine: 56 data bytes

64 bytes from name_of_machine (138.120.106.169): icmp_seq=0,
time=1. ms

64 bytes from name_of_machine (138.120.106.169): icmp_seq=1,
time=0. ms

64 bytes from name_of_machine (138.120.106.169): icmp_seq=2,

time=0. ms

^C

----name_of_machine PING Statistics----

3 packets transmitted, 3 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/0/1
```

If the packets were received out of order, if some packets were dropped, or if some packets took too long to complete the round trip, LAN congestion may be a problem. Contact your IT department or check physical LAN connectivity according to your company policy.

Procedure 7-3 Problem: Another machine can be pinged, but some functions are unavailable

Check the following to determine whether port availability or routing is the cause of management domain LAN issues:

- ports that need to be open across firewalls
- routing using netstat and ARP

1 The 5620 SAM uses numerous TCP and UDP ports for communication between various services. Some of these ports, such as the SNMP trap port, are configured during installation. Other ports are configured automatically by the software. Check that these ports are open or protected by a firewall, depending on system architecture needs.

The complete list of ports, their use, and the default port numbers are listed in the firewall section of the *5620 SAM Planning Guide*.

Note — Track any changes to port configuration values for future reference.

2 Run the following to check routing information.

i Open a DOS shell or command tool on the PC or workstation.

ii Run a trace route command to determine the path taken to a destination by sending an ICMP echo request message.

- Type tracert on a Windows PC
- Type traceroute on a Solaris workstation

The path displayed is the list of near-side interfaces in the path between a source host and a destination machine. The near-side interface is the interface closest to the source host.

iii Run the netstat -r and arp -a commands to display active TCP connections, Ethernet statistics, the IP routing table, and the ports on which the PC or workstation is listening.

Procedure 7-4 Problem: Packet size and fragmentation issues

Large packet sizes from the managed devices are being dropped by intermediate routers because the packets exceed the device MTU or the devices are not configured to forward fragmented packets, causing resynchronizations to fail. The 5620 SAM-managed devices are configured to send SNMP packets of up to 9216 bytes. The 5620 SAM is typically configured to accept large SNMP packets.

However, the typical L2 or L3 interface MTU on a 5620 SAM-managed device is likely configured to transmit smaller SNMP packets, usually in the 1500-byte range. This causes packet fragmentation. In order to handle these fragmented packets, intermediate devices between the 5620 SAM- managed device and 5620 SAM must be configured to handle or forward fragmented packets. When an intermediate network device, such as a router, cannot handle or forward fragmented packets, then packets may be dropped and resynchronization may fail. Consider the following.

- Enure that the CPM filters on managed devices are configured to accept fragmented packets, and that this filter policy is configured on each server in a redundant 5620 SAM deployment.
- Ensure that devices located between the managed devices, such as the 7750 SR, and the 5620 SAM can handle an MTU size of 9216 bytes, can fragment large SNMP packets, or can forward fragmented L2 or L3 packets.
- Verify the MTU packet sizes for all LAN devices.
- Verify that large packets can travel from the managed devices to the 5620 SAM by using CLI to ping the IP address of the 5620 SAM server, with a large packet.
- Ensure that the firewalls between the managed devices and the 5620 SAM server are configured to allow traceroute and ping packets.

1 Log in to the 7750 SR or another 5620 SAM-managed device.

2 Run the traceroute command:

> traceroute *SAM_server_IP_address* ↵

A list of hops and IP addresses appears.

3 Ping the first hop in the route from the managed device to the 5620 SAM server:

> ping *intermediate_device_IP_address* size 9216 ↵

A successful response indicates that the intermediate device supports large SNMP packets or packet fragmentation.

4 Repeat for all other hops until a ping fails or until a message indicates that there is an MTU mismatch. A failed ping indicates that the intermediate device does not support large SNMP packets or packet fragmentation.

5 Check the configuration of the intermediate device, and configure fragmentation or enable a larger MTU size.

8 — Troubleshooting Solaris and Windows platforms

8.1 Troubleshooting Solaris platforms

The following procedures describe how to troubleshoot Solaris platform workstation issues.

Procedure 8-1 Problem: Slow processing on a Solaris workstation and CPU peaks

The workstation is taking too long to perform a task. Check the CPU status to ensure that one process is not using most of the CPU cycles. Then use the mpstat and ps commands to further review CPU usage data.

When CPU usage remains high, and performance suffers, contact your Alcatel-Lucent support representative. Provide the data collected in this procedure.

You can also perform other procedures:

- If you are you performing a large listing operation using the 5620 SAM client GUI or OSS, check the LAN throughput using the netstat command, as described in Procedure 9-3.
- Check for excess disk usage using the vmstat command, as described in Procedure 8-3.

1 Open a command or shell tool.

2 Change to the 5620 SAM installation directory by typing:

cd /*installation_directory* ↵

where *installation_directory* is the installation directory of the 5620 SAM software

3 Run the prstat command to check for processes that are consuming CPU cycles:

i To list the top CPU processes using the UNIX utility prstat, type:

prstat ↵

Depending on your system configuration, approximately the top 20 processes are displayed.

ii Review the output.

The top 5620 SAM process listed under the CPU column should be the Java process. However, the Java process should not be consuming too much CPU. Some Oracle processes could also take CPU time, depending on the database load.

iii Press ESC-Q to quit or CTRL-C to stop the top command.

4 Use the UNIX utility mpstat command to further review the activities performed by the CPU.

i Type:

mpstat *time* ↵

where *time* is the interval, in seconds, that is monitored by the mpstat command

The *time* interval should be at least 10 s. An interval of more than 60 s may have an effect on applications because of the amount of time the system spends collecting mpstat data.

ii Review the mpstat output.

The following shows a sample mpstat output. See Table 8-1 for a description of the report.

```
CPU minf mjf xcal  intr ithr  csw icsw migr smtx  srw syscl
usr sys  wt idl

 0    1   0 5529   442  302  419  166   12  196    0   775
95   5   0   0

1    1   0  220   237  100  383  161   41   95    0   450   96
4    0   0

4    0   0   27   192  100  178   94   38   44    0   100   99
1    0   0

 5    1   0  160   255  100  566  202   28  162    0  1286
87   8   0   5
```

Table 8-1 mpstat report description

Heading	Description (events per second unless noted)
CPU	Processor identification
minf	Minor faults
mjf	Major faults
xcal	Interprocessor cross-calls
intr	Interrupts
ithr	Interrupts as threads (not counting clock interrupts)
csw	Context switches When the csw number slowly increases and the platform is not I/O bound, a mutex contention is indicated
icsw	Involuntary context switches When the iscw number increases beyond 500, the system is considered to be under heavy load
migr	Thread migrations to another processor
smtx	Spins on mutexes (lock not acquired on first try) if the smtx number increases sharply, for instance from 30 to 300, a system resource bottleneck is indicated

(1 of 2)

Heading	Description (events per second unless noted)
srw	Spins on readers/writer locks (lock not acquired on first try)
syscl	System calls
usr	Percent user time
sys	Percent system time
wt	Percent wait time
idl	Percent idle time

(2 of 2)

Review the usr, sys and idl data. Together, these three outputs indicate CPU saturation. A Java application fully using the CPUs should fall within 80 to 90 percent of the usr value, and 20 to 10 percent of the sys value. A smaller percentage for the sys value indicates that more time is being spent running user code, which generally results in better execution of the Java application.

As well, when the smtx output is high on a multiple CPU system, this indicates that CPUs are competing for resources.

iii Press ESC-Q to quit or CTRL-C to stop the mpstat command.

5 If processes are competing for CPU resources, you can isolate the information about a single process using the ps command.

i Check the state of CPUs by typing:

```
/usr/ucb/ps -aux ↵
```

A list of processes appears.

ii Review the ps output.

For CPU troubleshooting, the important data is listed in the %CPU row. If a process is taking 90% or more of the CPU resources, there may be a problem with the process. Contact your account or technical support representative for more information.

iii Press ESC-Q to quit or CTRL-C to stop the ps command.

Procedure 8-2 Problem: Slow performance on a Solaris workstation, but no spike or peak in the CPU

A platform is disk or I/O bound when it continuously services requests for data from a disk, and other activities must wait for those requests to complete. You can determine whether a machine is disk or I/O bound using the iostat command. You can also perform the following procedures:

When a disk is I/O bound and performance suffers, contact your Alcatel-Lucent support representative. Provide the data collected in this procedure.

- If the sluggish performance is not isolated using the iosat command, use the vmstat command in Procedure 8-3.
- Perform the 5620 SAM client GUI or OSS application procedures in chapter 9.

1 Open a command or shell tool.

2 To collect data to determine whether there is a disk bottleneck, type:

iostat -x *time* ↵

where *time* is the time, in seconds, over which you want to collect data. Alcatel-Lucent recommends that you start with 2 s.

To stop the iostat command, press CTRL-C.

3 Review the iostat output. The following is a sample of iostat data. See Table 8-2 for a description of the iostat report.

```
                          extended disk statistics

disk      r/s  w/s   Kr/s   Kw/s  wait actv  svc_t  %w  %b

sd1       0.1  0.2    0.9    3.3   0.0  0.0   34.3   0   0

sd3       0.1  0.5    1.1    3.7   0.0  0.0   73.1   0   90

                          extended disk statistics

disk      r/s  w/s   Kr/s   Kw/s  wait actv  svc_t  %w  %b

sd1       0.0  0.0    0.0    0.0   0.0  0.0   0.0   0   0

sd3       0.0  0.0    0.0    0.0   0.0  0.0   0.0   0   1
```

Table 8-2 iostat report description

Heading	Description
disk	Name of the disk
r/s	Reads per second
w/s	Writes per second
Kr/s	Reads per second (kb/s)
Kw/s	Writes per second (kb/s)
wait	Average number of transactions waiting for service (queue length)
actv	Average number of transactions actively being serviced (removed from the queue but are not yet complete)
svc_t	Average service time in ms
%w	Percentage of time there are transactions waiting for service (non-empty queue)
%b	Percentage of time the disk is busy (transactions in progress)

The %b and svc_t columns are the key fields to determine whether a disk bottleneck exists. If the average service time (svc_t) is between 30 and 50 ms, and the disk (%b) is greater than 20% busy, there is a minor disk loading problem. If the service times exceed 50 ms, the disk is considered disk or I/O bound.

In the example, the sd3 disk showed 90 percent disk activity in the %b column. Because disk sd3 is busier than disk sd1, disk performance may be enhanced by moving data from disk sd3 to disk sd1.

Procedure 8-3 Problem: There is excess disk activity on my Solaris platform

In a system with memory bottlenecks, there is a lot of disk activity. Much of this activity is related to swapping processes in and out of main memory. Swapping is detrimental to performance because it increases activity without contributing to productivity. This causes sluggish performance.

Swapping occurs when the active parts of the processes need more memory than the size of actual memory installed. When this happens, some of the memory contents are copied to disk and replaced by another process. When the portion of memory that was copied to disk is required, it is reloaded.

This scenario may continue until the system is no longer running any processes and is spending almost all of its time copying code and data in and out of main memory.

1 Open a command or shell tool.

2 To collect data, type:

vmstat *s* ↵

where *s* is the time, in seconds, over which you want to collect data. Alcatel-Lucent recommends that you start with 2 s.

3 Review the vmstat output. The following is a sample of vmstat data. See Table 8-3 for a description of the vmstat report.

```
#vmstat 2

procs     memory         page            disk         faults      cpu

r b w   swap  free   re mf pi po fr de sr s1 s3 - - in sy cs us sy id

0 0 0  45148 16628 0  6  3  1  3  0  1  0  1  0 0 89 473 192 1 1 98

0 0 0 527060 20548 0  7  0  0  0  0  0  0  0  0 0 73 280 143 0 0 99

0 0 0 527060 20548 0  0  0  0  0  0  0  0  0  0 0 18 319 143 0 0100
```

Table 8-3 vmstat report description

Heading	Description	Subheading
procs	Number of processes in each of the processor states	r - in run queue b - blocked for resources (I/O, paging) w - runnable but swapped
memory	Virtual and real memory usage	swap - amount of swap space currently available (kbytes) free - size of free space available (kbytes)
page	Page faults and paging activities in units per second	re - page reclaim mf - minor fault pi - kb paged in po - kb paged out fr - kb freed de - anticipated short-term memory shortfall (kbytes) sr - pages scanned by clock algorithms
disk	Number of disk operations per second	There are slots for up to four disks, labeled with a single letter and number. The letter indicates the types of disk: s = SCSI, i = IP; the number is the logical unit number.
faults	Trap or interrupt rates per second	in - (non-clock) device interrupts sy - system calls cs - CPU context switches
cpu	Breakdown of percentage usage of CPU time. On multiple processor systems, this is an average for all processors.	us - user time sy - system time id - idle time

4 Review the results.

The sr column under the disk heading shows the scan rate. The scan rate is the key factor because it indicates how often the system scans memory for idle pages to swap out. When the scan rate is zero, there is no swap problem. The higher the scan rate, the more time the system is spending copying code and data in and out of memory.

Check the memory swap and free columns. When there is little or no available free memory, you need more swap space.

You can add swap space to resolve memory bottleneck problems and improve performance. Contact your technical support representative for information about adding new disks to provide the necessary swap space to stop memory bottlenecks. Perform Procedure 8-4 to add emergency swap space to provide a temporary solution.

Check the minimum supported platform size for the software to ensure enough swap space is allocated.

5 To stop the vmstat command, press CTRL-C.

Procedure 8-4 Problem: There is not enough swap space added or the Solaris platform is disk bound

You can add swap space to improve memory performance. For a more permanent solution, add more RAM. Use this procedure when:

- insufficient disk space causes memory performance issues
- insufficient swap space was installed, or the network load requires more swap space

When you allocate a file to be used as emergency swap space, the amount of swap space available increases without reformatting a disk.

Note — Before creating a new swap file, run the swap -l and swap -s commands to determine how much disk space is currently allocated. Then perform the swap -s command after creating a new swap file to verify that the new emergency swap space was correctly allocated.

1 As root, type:

`df -k` ↵

The displayed information lists the capacity and usage of the available disk space. Determine where there is enough disk space to create a swap file.

2 Change directories by typing:

`cd /`*`swapdirectory`* ↵

where *swapdirectory* is the name of the directory where you are going to create a new swap file

3 Create a new swap file by typing:

`mkfile` ***`swapfilesize`*`m`** ***`swapfilename`*** ↵

where
swapfilesize is the size of the swap file you are creating. The size of the *swapfilesize* is followed by an m to denote Mbytes.
swapfilename is the name of the swap file you are creating

4 The vfstab file controls which partitions are mounted. Edit the vfstab file:

i Use a text editor, such as vi or textedit, to edit the vfstab file by typing:

`vi /etc/vfstab` ↵

ii Move the cursor to the last line in the vfstab file and type:

```
/swapdirectory/swapfilename - - swap - no -
```

where
swapdirectory is the name of the directory where you created the new swap file
swapfilename is the name of the swap file you created

iii Save the changes and quit the text editor.

5 To allocate the emergency swap file, type:

swap -a /*swapdirectory*/*swapfilename* ↵

where

swapdirectory is the name of the directory where you created the new swap file

swapfilename is the name of the swap file you created

6 Verify that the swap file is allocated by typing:

swap -l ↵

and

swap -s ↵

Several lines are displayed. The format of the last line is:

```
total: 52108k bytes allocated + 24944k reserved = 77052k used,
93992k available
```

8.2 Troubleshooting Windows platforms

Many of the commands in section 8.1 and throughout the rest of the *5620 SAM Troubleshooting Guide* can also be performed on a Windows platform PC. In all cases, the commands are run from the DOS command line. As well, you can check PC performance and running process details using the Task Manager. Some of the commands include:

- ping
- tracert
- taskmgr (Task Manager)
- ipconfig

The Windows Task Manager provides details about programs and processes that run on the PC. If you are connected to a LAN, you can also view network status and check network performance. Depending on the NOC work environment and shared computer usage policy, you can also view additional information about other users.

Use your PC and Windows operating procedure manuals, or check with the IT department, for information about stopping programs or processes, starting programs, and viewing the dynamic display of computer performance using the Task Manager.

9 — Troubleshooting 5620 SAM clients

9.1 Troubleshooting common client application problems

The following procedures describe how to troubleshoot 5620 SAM GUI and OSS client application issues.

Procedure 9-1 Problem: Cannot start 5620 SAM client, or error message during client startup

Check the following:

- the 5620 SAM client and server have the same software versions and compatible patch sets
- the login name and password of the user are correct
- there are no UNIX errors
- the correct 5620 SAM license key is installed
- a local firewall is running on the PC client

1 If the 5620 SAM client is installed on UNIX or Solaris and you receive a “Cannot execute” message when you try to run the client, the client executable file permission may have been reset by an event such as an auto-client update failure. Perform the following steps to correct this.

i Log in as a root-equivalent user, or as the user that installed the 5620 SAM client, on the client station.

ii Open a console window.

iii Enter the following at the CLI prompt to set the execute-permission flag on the client executable file:

chmod +x *path*/nms/bin/nmsclient.bash

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

2 Review the login pop-up messages that appear when a client GUI attempts to connect to a server. Messages that state things like the server is starting or the server is not running indicate the type of communication problem.

3 To check that the login name and the password of the user are correct, modify the login and password as 5620 SAM admin and have the user attempt to log in.

i Start the 5620 SAM client as the admin user.

ii Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The Security Management (Edit) form appears with the General tab displayed.

iii Click on the Users tab button.

iv Configure the list filter criteria and click on the Search button. A list of users is displayed.

v Select a user.

vi Click on the Properties button. The User (Edit) form appears.

vii Enter a new password for the User Password parameter.

viii Confirm the password for the Confirm Password parameter.

ix Click on the Apply button to save the changes.

x Have the user attempt to start a 5620 SAM client and log in.

4 To check that the 5620 SAM server is up and to view additional server configuration information, perform the following steps.

i Log on to the 5620 SAM server station as an administrative user.

> **Note —** If the 5620 SAM server is installed on Solaris, you must log in as the samadmin user.

ii Open a console window.

iii Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/bin on Solaris or C:\5620sam\server\bin on Windows.

iv If the 5620 SAM server is installed on Solaris, enter the following at the CLI prompt:

./nmsserver.bash appserver_status ↵

Server status and configuration information are displayed.

v If the 5620 SAM server is installed on Windows, enter the following at the CLI prompt:

nmsserver.bat appserver_status ↵

Server status and configuration information are displayed.

vi To check additional server status conditions, perform Procedure 10-1.

5 Check the license key.

When an incorrect license key is installed on the 5620 SAM, the client GUI does not start, even when the correct user account name and password are used. When the 5620 SAM server does not start because of license key issues, perform Procedure 10-9. Ensure that the license key matches the load installed. For example, you cannot use a Release 7.0 license key with 5620 SAM Release 8.0 software.

6 Check the client GUI login error message.

When a firewall is running locally on the PC client where the 5620 SAM client is installed, a login error message may appear indicating that the server is not available. Ensure that a local firewall is not preventing a connection to the server, and that the 5620 SAM server IP address is in the client host-lookup file.

Procedure 9-2 Problem: 5620 SAM client unable to communicate with 5620 SAM server

Before you proceed, ensure that the following conditions are present.

- The 5620 SAM client points to the correct IP address and port of the server.
- The problem is not a network management domain LAN issue. See chapter 7 for more information.
- Firewalls between the 5620 SAM clients and the server are correctly configured

1 To check that the 5620 SAM client points to the correct IP address and port of the server, open the nms-client.xml file using a text editor. The default file location is *installation_directory*/nms/config.

where *installation_directory* is the directory in which the 5620 SAM client software is installed, for example, /opt/5620sam/client

2 Verify the IP address of the server as specified by the ejbServerHost parameter.

3 Verify the server port as specified by the ejbServerPort parameter.

4 Modify the IP address and port values, if required.

5 Save the file, if required.

6 Perform Procedure 10-1 to check the server status. A client cannot connect to a 5620 SAM server that is not started.

7 If the server is started, compare the firewall and network configuration guidelines in the *5620 SAM Planning Guide* to with your network configuration to ensure that it complies with the guidelines.

8 Contact your Alcatel-Lucent support representative if the problem persists.

Procedure 9-3 Problem: Delayed server response to client activity

Possible causes are:

- a congested LAN
- improperly sized platforms

Using the netstat command on the client may help troubleshoot network throughput problems. When an Ethernet LAN is highly congested, the actual throughput slows down. This is caused by packets colliding on the LAN as multiple machines begin to transmit at approximately the same time, for example, when multiple 5620 SAM client GUIs or OSS applications are performing simultaneous tasks.

1 Client GUI windows may respond more slowly than normal during resynchronizations of managed devices. Repeat the client GUI window action when the resynchronization is complete.

2 Check for LAN throughput issues.

i Open a shell console window.

ii Enter the following at the console prompt to display local network-interface transmission data over a period of time:

netstat -i *s* ↵

where *s* is the time, in seconds, over which you want to collect data. Alcatel-Lucent recommends that you start with 50 s

iii Review the output. The following is sample netstat output:

```
netstat -i 5

 input   le0       output          input  (Total)    output

packets errs  packets errs  colls packets errs  packets errs
colls

6428555 41    541360  80    49998 6454787 41    567592  80
49998

22      0     0       0     0     22      0     0       0     0

71      0     7       0     3     71      0     7       0     3
```

This sample displays the number of input and output packets, errors and collisions on the le0 interface. One column displays the totals for all interfaces. This sample only has one interface, so both sets of columns display the same data.

Calculate the number of collisions as a percentage of the number of output packets. For example, according to the last line of output, there were three collisions and seven output packets resulting in a 42% rate.

This number is high, but the time in which the sampling was obtained (5 s), was low. Change the sample rate to, for example, 50 s for an accurate sampling of the network throughput.

When collisions are between 2% and 5%, congestion on the interface is within the normal operating range.

In a typical network, when collisions are greater than 5%, you may have a serious congestion problem on the interface. Review your LAN topology and design to reduce the number of network bottlenecks.

iv To stop the netstat command, press CTRL-C.

3 Check that the client platform is appropriately sized. See the *5620 SAM Planning Guide* for more information.

Procedure 9-4 Problem: Cannot view 5620 SAM alarms using 5620 NM client

Possible causes include incorrectly configured param.cfg parameters on the 5620 NM to allow the forwarding of alarms to those platforms from the 5620 SAM.

1 Open a command tool on the 5620 NM client station.

2 Navigate to the AS tool IM directory by typing:

`/opt/netmgt/ALMAP/as/data/ascurim_0` ↵

3 Open the param.cfg file.

4 Ensure the NSP_USE_NSP and CORBA_SERVER_DISCOVERY parameters are set to True.

5 Save the changes and close the file.

6 When the filters for CORBA are set to True, ensure the CORBA filter files are set correctly. Navigate to the AS tool IM configuration directory by typing:

`/opt/netmgt/ALMAP/as/data/ascurim_0/ASIMconfig` ↵

7 Ensure the following filters are set in the ASIMconfig or ASIMFilter files:

```
CORBA_ROOT_NAME_FILTER="*/*/AlarmSynchronizer*";

CORBA_ROOT_NAME_FILTER="*/*/EventChannelFactory*";

CORBA_ROOT_NAME_FILTER="*/*/X733EventChannel*";
```

8 Save the changes and close the file.

Procedure 9-5 Problem: Unable to print from Solaris platform client

Printers are connected to clients to provide a printed record of alarms, the GUI, or text files.

Note — Many printers have Ethernet connections. Troubleshooting these printers is beyond the scope of this document.

A common problem with printers is incorrect connections and configuration. Printers must be connected properly to the serial port of the workstation before you can print. See the Sun documentation and the printer documentation for more information about connecting printers.

If you are using a printer server, ensure that the printer is listed in the /etc/hosts file

Table 9-1 lists some common printer problems.

Table 9-1 Troubleshooting Solaris printer problems

Problem	Probable cause	Solution
A new user cannot print	No entry for that printer in the user account .cshrc file	Add an entry for printer to the .cshrc file (for Solaris)
The .cshrc file was changed, but the user still cannot print	Changes to the .cshrc file takes effect the next time the user logs out and logs back in	The user should log out and log back in
A user cannot delete a printer	There are print jobs in the queue for that printer	Delete the print jobs in the queue using the lprm command
The client cannot print	The printer was not added to the list of available printers	Add the printer to the list of printers by using the admintool

1 On the workstation, log in as the user experiencing printing problems.

2 Type the lp command that you want to use:

a To list jobs in the printer queue, type:

lpq ↵

When you run the lpq command and a message appears that the printer cannot be found, there is a connection problem between the PC or workstation and the printer. A printer cannot be found message may indicate that the environment variable for the printer is not set correctly, or that the machine is not configured to use the printer.

b To display information about the state of the printer, type:

lpstat ↵

When you run the lpstat command and a message appears that the printer cannot be found, there is a connection problem between the machine and the printer.

c To remove print jobs from the printer queue, type:

lprm ↵

Procedure 9-6 Problem: Cannot place newly discovered device in managed state

Possible causes are:

- a corrupt or incorrectly entered 5620 SAM server license key
- the 5620 SAM server license key is not for the correct hostid
- the number of managed cards (MDAs) exceeds the 5620 SAM server license
- another application using a port required by the 5620 SAM server
- resychnronization problems between the managed network and the 5620 SAM

See Procedure 10-9 for more information.

Procedure 9-7 Problem: I performed an action, such as saving a configuration, but I cannot see any results

Possible causes are:

- Failed SNMP communication between the server and managed device. See Procedure 10-8 for more information.
- Failed deployment of the configuration request.

1 For the 5620 SAM client, perform the following:

i Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu.

The Deployment form opens with the Incomplete Deployments tab displayed. Incomplete deployments are listed, and deployer, tag, state and other information is displayed. The possible states for a deployment are:

- Deployed
- Not Deployed
- Pending
- Failed — Resource Unavailable. Failure occurred because one of the resources required to apply the configuration is not present in the 5620 SAM database
- Failed — Configuration. Failure occurred because the configuration could not be applied to the specified objects
- Failed — Partial. Failure occurred at deployment and some of the configuration can been sent to the network
- Failed — Internal Error. Failure a occurred due to general error conditions. Code is intended as a catch-all code for all other possible errors
- Cancelled
- Postponed

You can also suspend or resume deployment retries by clicking on the Suspend Retries or Resume Retries button. You can clear a deployment by clicking on the Clear button. When you clear a deployer, no further attempt is made to reconcile the network device status with the 5620 SAM database. Affected objects should be resynchronized.

If a deployment is not sent to a managed device, the intended configuration change is not made on the device.

ii Choose a failed deployment and click on the Properties button to view additional information. The deployment properties form opens.

2 When a deployment fails and you receive a deployment alarm, check the following:

i Using CLI, check on the device whether the deployment change is on the device.

ii If the change is on the device, the deployment alarm was likely raised because the configuration already exists on the device. Clear the failed deployment and resynchronize the device with the 5620 SAM.

If the change is not on the device, collect the information from the deployment properties form and contact your Alcatel-Lucent support representative.

3 For client OSS applications, perform the following:

Note — These steps describe how to troubleshoot asynchronous deployment requests only. Alcatel-Lucent recommends that deployment requests be made in asynchronous mode.

i Browse real-time alarms received via JMS. An alarm denoting a deployment failure contains the following text:

```
Attribute: alarmClassTag Value: generic.DeploymentFailure
```

The alarm also contains additional information, including the object affected by the alarm and the severity of the alarm. See the *5620 SAM-O OSS Interface Developer Guide* for more information.

ii Find the following text in the alarm:

`Attribute: requestID=`*`requestID`*

The parameter specifies the request id sent with the original request. The request id should be unique per request.

iii Determine the original request using the request id.

iv Troubleshoot the original request. If there are problems with the original request, clear the deployer, fix the request, and send the new request. See the *5620 SAM-O OSS Interface Developer Guide* for more information.

v If there are no problems with the original request, the failure may be caused by a network communication or device failure, or by packet collisions caused by conflicting configurations. You can:

- resend the request
- troubleshoot your network or device

Procedure 9-8 Problem: Device configuration backup not occurring

1 Use the 5620 SAM client to check the device database backup settings. Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens with the Backup/Restore Policy tab displayed.

2 Click on the Backup/Restore Status tab button. The managed devices are listed and backup and restore status information is displayed.

3 Select the device and click on the Properties button. The NE Backup/Restore Status form opens with the General tab displayed.

4 View the information in the Backup Status panel. A Backup State other than Successful may indicate a communication problem or a backup policy configuration error.

5 Ensure that the device configuration file and the associated index file are saved on the device and available for backup. Click on the Configuration Saves tab button, and ensure that the Config Save State indicator reads Success.

See the appropriate device operating-system documentation for more information.

6 Click on the Backups tab button to view a list of backup operations that are currently in progress. A backup operation disappears from the list after it completes.

7 Click on the Faults tab to view additional troubleshooting information.

8 Close the NE Backup/Restore Status form.The Backup/Restore form is displayed.

9 Use the information obtained from the NE Backup/Restore Status form to check the backup policy configuration, if required. Click on the Backup/Restore Policy tab button.

10 Select the backup policy for the device and click on the Properties button. The Backup Policy (Edit) form opens with the General tab displayed.

11 Ensure that the policy is assigned to the device.

- **i** Click on the Backup/Restore Policy Assignment tab button.
- **ii** If required, configure a filter and click on the OK button.
- **iii** Move the device to the Assigned Sites list if it is not there by selecting the site from the Unassigned Sites list and clicking on the right-arrow button.
- **iv** Click on the Apply button to save changes, as required.

12 Click on the General tab button.

13 Verify the parameter settings and modify, if required.

14 Click on the OK button to save the changes and close the form.

9.2 Troubleshooting client GUI issues

The following procedures describe how to troubleshoot client GUI-specific issues.

Procedure 9-9 Problem: 5620 SAM client GUI shuts down regularly

The 5620 SAM client GUI automatically shuts down under the following conditions:

- no activity on the GUI for a specified amount of time
- no communication between the GUI and the server for a specified amount of time.
- when there is an communication error that causes problems between the server and the client

Note — Changing the OS clock setting on the server station can cause communication problems on the client. If the server clock setting changes significantly, the clients must log off and the server must be restarted. Alcatel-Lucent recommends that the server OS clock be tied to a synchronous timing source to eliminate time shifts that may lead to polling and communication problems.

1 Disable the GUI activity check, if required. Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The Security Management (Edit) form appears with the General tab selected.

2 Set the Client Timeout (minutes) parameter to 0 to disable the GUI inactivity check. Alternately, you can configure a higher value for the parameter, to increase the time that must pass before the client GUI is shut down due to inactivity.

3 Click on the Apply button and close the form.

Procedure 9-10 Problem: Configuration change not displayed on 5620 SAM client GUI

The 5620 SAM supports the configuration of certain complex objects, such as services, using a sequence of configuration forms and steps or templates. Additional configuration forms and steps may be contained within the main, or parent, configuration form. For example, when you configure a VLL service, a site configuration form is contained within the main configuration form. In turn, an L2 interface configuration form is contained within the site configuration form. Alternately, when you use service templates, parent templates for site configuration must also be configured.

Objects configured in contained configuration forms are not saved until the parent configuration form is saved. For example, when you configure a VLL service, sites or L2 interfaces that you configure are not saved during service creation until the parent configuration form is saved. You cannot view new objects or new object configurations in other parts of the GUI, such as the equipment window, until the service is saved.

The 5620 SAM displays a dialog box to indicate that configured objects in a configuration form are not saved until the parent configuration forms are saved.

Procedure 9-11 Problem: List or search function takes too long to complete

You can perform simple listings or complex searches using the Manage menu on the 5620 SAM main menu to query the database for information about services, customers, and other managed entities.

Depending on the type of information and the number of entries returned, a list or search operation may take considerable time to complete. As a general rule, Alcatel-Lucent recommends that you use filters to restrict the number of items in a list or search operation to 10 000 or fewer.

See the 5620 SAM User Guide for information about the 5620 SAM client GUI list and search functionality. See the *5620 SAM Planning Guide* for information about 5620 SAM scalability and system capacity guidelines.

Procedure 9-12 Problem: Cannot select certain menu options or cannot save certain configurations

The 5620 SAM allows the administrator to restrict access to parts of the GUI, or restrict the ability of a user to configure objects or save configurations. Check with your administrator to determine your permissions and scope of command.

When an administrator changes user or user group permissions from the 5620 SAM security menus, the changes take effect immediately and determine the actions that a user can perform from the client GUI.

As well, the license key must enable the appropriate software module to perform a certain function. For example, if the 5620 SAM-P module is not installed or licensed, you cannot use the GUI to create a service. See Procedure 10-9 for more information about viewing license keys to determine what modules are installed.

Procedure 9-13 Problem: Cannot clear alarms using 5620 SAM client GUI

If you cannot clear alarms, there may be an underlying database issue. Collect the logs outlined in Procedure 2-1 and contact your Alcatel-Lucent support representative.

Procedure 9-14 Problem: Cannot open user documentation from 5620 SAM client GUI

When the 5620 SAM client GUI cannot find a browser to launch the user documentation index file, it generates an error message indicating that no browser is available. There are multiple ways to fix this problem.

1 Note the location of the user documentation directory index.html file from the error message.

2 Perform one of the following:

a Launch your own browser to view the index.html page. When you launch your own browser on the client GUI, you cannot use the Help menu link.

i Launch a browser.

ii Copy the URL from the error message into the browser address line. The index.html file appears.

iii Navigate to the appropriate documentation.

b Update the nms-client.xml file to indicate a browser location. The 5620 SAM then uses that location to launch a browser.

i Go to the *installation_directory*/nms/config directory.

where *installation_directory* is the directory in which the 5620 SAM client software is installed, for example, /opt/5620sam/client

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

iii Add the following tag within the <configuration> tag.

```
<documentation>

application="full_path_to_browser_executable"

</documentation>
```

iv Restart the client GUI.

v Launch the documentation from the client GUI Help main menu. The browser appears with the index.html page displayed.

c Avoid using a browser. Navigate to the folder or directory in which the documentation PDF files are stored.

On a Solaris station, the location is typically /opt/5620sam/client/nms/distribution/User_Documentation.

On a Windows station, the location is typically C:\5620sam\client\nms\distribution\User_Documentation.

Procedure 9-15 Problem: The 5620 SAM client GUI does not display NE user accounts created, modified, or deleted using the CLI

When a NE user account is created, modified, or deleted using the CLI, the 5620 SAM client GUI does not update the user list in the NE User Profiles form. For increased security, the node does not send a trap for changes made to node user accounts. You can align the 5620 SAM client GUI with the node user account changes by resynchronizing the node.

1 Choose Equipment from the 5620 SAM navigation tree drop-down menu.

2 Navigate to the NE. The path is Network→NE.

3 Right-click on the NE and choose Resync.

The Resync menu option specifies that SNMP MIB and CLI information bases are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.

10 — Troubleshooting 5620 SAM server issues

10.1 Troubleshooting 5620 SAM server issues procedures

The procedures in this chapter describe how to troubleshoot 5620 SAM server issues.

Note — 5620 SAM server statistics collection is a useful troubleshooting tool for memory-, alarm-, and SNMP-related issues on the 5620 SAM servers. See the *5620 SAM Statistics Management Guide* for more information.

Procedure 10-1 Problem: Cannot start a 5620 SAM server, or unsure of 5620 SAM server status

The 5620 SAM main or auxiliary server startup script provides server status indicators that include the following:

- how long the server has been running
- the used and available memory
- the database connectivity status
- 5620 SAM license capacity

1 Log in to the 5620 SAM server as an administrator.

Note — If the 5620 SAM server is installed on Solaris, you must log in as the samadmin user.

2 Open a console window.

3 To check the status of a 5620 SAM main server, perform the following steps.

i If the 5620 SAM main server is installed on Solaris, enter the following at the CLI prompt:

***path*/nms/bin/nmsserver.bash appserver_status** ↵

where
path is the 5620 SAM server installation location, typically opt/5620sam/server

The general 5620 SAM server application status is displayed.

ii If the 5620 SAM main server is installed on Solaris, enter the following at the CLI prompt:

***path*/nms/bin/nmsserver.bash nms_status** ↵

where
path is the 5620 SAM server installation location, typically opt/5620sam/server

Detailed 5620 SAM server information is displayed.

iii If the 5620 SAM main server is installed on Windows, enter the following at the CLI prompt:

***path*\nms\bin\nmsserver.bat appserver_status** ↵

where
path is the 5620 SAM server installation location, typically C:\5620sam\server

The general 5620 SAM server application status is displayed.

iv If the 5620 SAM main server is installed on Windows, enter the following at the CLI prompt:

***path*\nms\bin\nmsserver.bat nms_status** ↵

where
path is the 5620 SAM server installation location, typically C:\5620sam\server

Detailed 5620 SAM server information is displayed.

v To obtain more specific server status information, run the nmsserver script in step 3 using the appropriate option from Table 10-1 in place of the nms_status or appserver_status option.

Table 10-1 5620 SAM main-server startup script options

Option	Description
start	Starts the 5620 SAM main server in noninteractive mode on a Solaris workstation or in interactive mode on a Windows PC
stop	Stops the 5620 SAM main server
appserver_status	Returns information about the status of the 5620 SAM main server (both active and standby servers when the 5620 SAM is configured for redundancy)
appserver_version	Returns build information, including the start date of the current instance of the 5620 SAM main server
nms_status	Returns the following information: • 5620 SAM standalone, primary, or standby server start time and running time • total used and available memory • database connectivity status • redundancy configuration and status • 5620 SAM license information • JVM memory-usage information • alarm forwarding information • basic auxiliary server information • number and status of current process threads
-v nms_status	Verbose version of the nms_status option that returns the following additional information: • ID and status of the current process threads • general JMS server information • currently connected JMS subscribers, by topic

(1 of 2)

Option	Description
nms_info	Returns the following information from the 5620 SAM database: • number of managed devices by device type; for example, 7750 SR • number of MDA ports by type • number of equipped ports by type • number of services by type; for example, IES or VLL • number of access interfaces, connection termination points, and channels, by type • number of alarms, listed in order of severity • lists of enabled statistics, file, and accounting policies, including the counts and the polling frequency for different types of objects
nms_version	Returns the build identifier (base release and patch version) of the installed 5620 SAM server software
jvm_version	Returns version information about the currently running Java Virtual Machine environment
script_env	Returns main server script environment information
read_config	Rereads the nms-server.xml server configuration file while the server is running. This allows you to update server parameters without stopping the server, for example, to update alarm agent settings or to update the managed MDA license capacity.
force_restart	Forces the 5620 SAM main server to restart
force_stop	Forces the 5620 SAM main server to stop
passwd <*username*> <*current*> <*new*> where *username* is the database username, for example, samuser *current* is the current password *new* is the new password	Changes the database user password
jmsstart	Starts the JMS server in interactive mode
jmsstop	Stops the JMS server
jmsappserver_status	Returns JMS server status information
jmsstatus	Returns information that includes the following: • general JMS server information • currently connected JMS subscribers, by topic
jmsjvm_version	Returns version information about the currently running Java Virtual Machine environment
jmsscript_env	Returns JMS server script environment information
jmsread_config	Rereads the JMS server configuration file while the JMS server is running
jmsforce_restart	Forces the JMS server to restart
no keyword, help, or ?	Lists the available command options

(2 of 2)

4 To check the status of a 5620 SAM auxiliary server, perform the following steps.

i Enter the following at the CLI prompt:

***path*/nms/bin/auxnmsserver.bash aux_status** ↵

where
path is the 5620 SAM server installation location, typically opt/5620sam/auxserver

The general 5620 SAM server application status is displayed.

ii Enter the following at the CLI prompt:

***path*/nms/bin/auxnmsserver.bash auxappserver_status** ↵

where
path is the 5620 SAM server installation location, typically opt/5620sam/auxserver

Detailed 5620 SAM server information is displayed.

iii To obtain more specific server status information, run the nmsserver script using the appropriate option from Table 10-2 in place of the aux_status or appserver_status option.

Table 10-2 5620 SAM auxiliary-server startup script options

Option	Description
auxappserver_status	Returns information about the operational status of the auxiliary server
auxdebug	Starts the auxiliary server in interactive mode
auxforce_restart	Forces the auxiliary server to restart
auxforce_stop	Forces the auxiliary server to stop
auxjvm_version	Returns the auxiliary server JVM version
auxread_config	Directs the auxiliary server to read and apply the settings in the general configuration file
auxread_metrics_config	Directs the auxiliary server to read and apply the settings in the metrics configuration file
auxscript_env	Returns auxiliary server script environment information
auxstart	Starts the 5620 SAM auxiliary server
auxstatus	Returns information about the auxiliary server that includes the following: • IP address • port number • database connections • installed server software build version
auxstop	Stops the 5620 SAM auxiliary server
aux_version	Returns the auxiliary server software version
auxhelp, *no keyword*, or ?	Lists the available command options

5 Review and record the displayed information for Alcatel-Lucent technical-support, if required.

6 Close the console window.

7 View the 5620 SAM server logs for error messages using the 5620 SAM LogViewer GUI application, as described in chapter 6.

8 Report the error messages that you find to an Alcatel-Lucent technical support representative.

Procedure 10-2 Problem: 5620 SAM server and database not communicating

Perform this procedure when a 5620 SAM server cannot connect to a 5620 SAM database.

1 Verify network connectivity between both the primary and standby servers and the primary and secondary databases by ensuring that both the primary and standby servers and the primary database can ping each other. See chapter 7 for more information.

2 Ensure that the ports specified at installation time are available and not being blocked by firewalls. See chapter 7 for more information.

3 Perform the following troubleshooting activities for the primary database, as described in Procedure 11-6.

- Verify the correct IP address and instance name of the database.
- Verify that the database instance is running.
- Verify that the database is running in the correct mode.

See the 5620 SAM Planning Guide for more information about the ports that must be available for the 5620 SAM to function. If the problem persists, collect the logs identified in Procedure 2-1 and contact your Alcatel-Lucent support representative.

Procedure 10-3 Problem: A 5620 SAM server starts up, and then quickly shuts down

When a server starts then stops, collect logs as described in Procedure 2-1 and contact your Alcatel-Lucent support representative.

Procedure 10-4 Problem: Client not receiving server heartbeat messages

Perform this procedure when a 5620 SAM client is not receiving heartbeat messages.

1 Verify network connectivity between both the primary and standby servers and the clients by ensuring that both the primary and standby servers and the clients can ping each other. See chapter 7 for more information.

2 Verify that the 5620 SAM server and client clocks are synchronized. To set the date and time for 5620 SAM server and client clocks, see the *5620 SAM Maintenance Guide* for more information.

Procedure 10-5 Problem: A 5620 SAM server cannot be reached over a network

Perform this procedure to check the IP connectivity between a 5620 SAM client and main server using ping commands. When the ping commands indicate that IP communication is active but there are still IP reachability issues, the problem could be poor LAN performance.

To test whether IP packets are arriving at the PC or workstation, whether packets are missing, or whether packets are slowed because of round-trip delays, use the ping -s command on a Solaris workstation or the ping *destination_IP_address* -t command on a PC. The ping -s command issues a number of sequentially ordered packets. Packets returned out of sequence indicate that there are LAN problems.

1 Perform a ping test to measure reachability, as described in Procedure 7-2.

2 On Solaris installations, If you cannot ping the 5620 SAM server, make sure that the host name of the server is in the /etc/hosts file.

  i Change to the /etc directory by typing:

  cd /etc ↵

  ii Open the hosts file with a text editor, such as vi or textedit.

  iii Add the host name and IP address of the 5620 SAM server. For example, type:

  123.456.789.10 station3

  where *123.456.789.10* is the IP address of the 5620 SAM server named *station3*

  iv Save the changes and close the file.

Procedure 10-6 Problem: Excessive 5620 SAM server-to-client response time

As the number of managed devices grows and as more GUI or OSS clients are brought online, the processing load on the 5620 SAM system increases. For optimum 5620 SAM performance, you must ensure that the 5620 SAM configuration meets the requirements in the *5620 SAM Planning Guide* as your network expands.

You can do the following to increase the available 5620 SAM server network management resources:

- Deploy the 5620 SAM system in a distributed configuration.
- Deploy the 5620 SAM system in a redundant configuration.
- Deploy 5620 SAM auxiliary servers.
- Reallocate the 5620 SAM server resources that are assigned to groups of managed devices.

See the *5620 SAM User Guide*, *5620 SAM System Architecture Guide*, and the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about a particular option. Contact Alcatel-Lucent support for reconfiguration assistance.

Perform this procedure to check the following:

- 5620 SAM auxiliary server status

  System performance may degrade if the number of available Preferred and Reserved auxiliary servers drops below the number of configured Preferred auxiliary servers.
- 5620 SAM main server status

  Alarms raised against the 5620 SAM main server may provide information about the performance degradation.

Caution — Only Alcatel-Lucent support staff are qualified to assess and reconfigure a 5620 SAM deployment.

1 Open a 5620 SAM client GUI.

2 Choose Administration→System Information. The System Information form opens.

3 Click on the Faults tab button to view auxiliary server and general 5620 SAM system alarm information, if required.

4 If your 5620 SAM deployment includes one or more auxiliary servers, perform the following substeps to check the status of each auxiliary server.

i Click on the Auxiliary Servers tab button.

ii Review the list of auxiliary servers.

iii Select an auxiliary server in the list and click on the Properties button. The properties form for the auxiliary server is displayed.

iv Review the information, which includes:

- the auxiliary server IP address
- the auxiliary server host name
- the auxiliary server port number
- the auxiliary server type (Reserved or Preferred)
- the auxiliary server status (Unknown, Down, Up, or Unused)

v If the auxiliary server status is Down, perform Procedure 10-1 on the auxiliary server.

vi If the auxiliary server status is Unknown, perform Procedure 10-11 to check the connectivity between the managed network and the main and auxiliary servers.

5 Close the System Information form.

Procedure 10-7 Problem: Unable to receive alarms on the 5620 SAM, or alarm performance is degraded

By default, the system begins purging alarms when the outstanding alarm count reaches 50 000, unless historical alarm record logging and purging alarm policies are configured to keep the outstanding alarm count below that level.

Caution — Exceeding the alarm limit configured in the nms-server.xml file may cause system performance problems.

1 Check the status bar of the 5620 SAM client GUI status bar for indications that the maximum number of alarms for the system is reached.

2 If required, clear outstanding alarms or delete them to the alarm history record log, as described in the *5620 SAM User Guide*.

3 If the 5620 SAM system includes one or more auxiliary servers, perform Procedure 10-6 to ensure that system performance is not degraded because of auxiliary-server unavailability.

4 Contact your Alcatel-Lucent support representative for more information.

Procedure 10-8 Problem: All SNMP traps from managed devices are arriving at one 5620 SAM server, or no SNMP traps are arriving

When you install the 5620 SAM server, you specify the port on which SNMP traps arrive. In addition, two sets of configurations must be completed for SNMP trap notifications to work:

- Enable key SNMP parameters on the devices before managing them.
- Ensure that a unique trapLogId is specified for each router to communicate with the 5620 SAM. If the trapLogId is used by other applications or by another 5620 SAM, traps may be misdirected or directed to only one machine.

Note — You must have sufficient user permissions, for example, admin permissions, to configure SNMP on a device.

1 See the commissioning chapter of the *5620 SAM User Guide* for more information about configuring devices for 5620 SAM management, including enabling the SNMP engine and defining at least one SNMP community.

2 Configure SNMP on the device using CLI.

Procedure 10-9 Problem: Cannot manage new devices

The possible causes are:

- An incorrect license key was entered or the license key is corrupt.
- The license key is not for the correct host ID.
- The number of managed cards (MDAs) exceeds the license key.
- The 5620 SAM-O cannot connect because the license key is not enabled for 5620 SAM-O
- Another application is using the port that is required by the 5620 SAM server.
- Large packet sizes from the managed devices are being dropped by intermediate routers because the packets exceed the device MTU, causing resynchronizations to fail.

Additional devices cannot be managed, but can be discovered, when the license key card (MDA) limit is exceeded. When an incorrect license key is entered during installation or the license key file is corrupt, you can correct it.

Caution — Do not modify other nms-server.xml parameters. Modifying the file can seriously affect network management and performance of the 5620 SAM.

1 Check the license-key status.

i The 5620 SAM generates an alarm when a license limit is exceeded or nearly exceeded. View the dynamic alarm list on the 5620 SAM client GUI, or the JMS real-time alarm feed from the 5620 SAM OSS client application for alarms related to nearing or exceeding a license limit.

ii Choose Help→5620 SAM License Information from the 5620 SAM client GUI main menu. The 5620 SAM License (View) form opens.

iii View the information in the Devices and Quantities Licensed panel and ensure that no Remaining quantity equals zero.

Note — If you have a new license key that supports a greater number of managed objects, you can dynamically update the license key without shutting down the server. See the *5620 SAM User Guide* for information about changing a 5620 SAM license key.

2 Specific ports need to be available for the 5620 SAM server. Check the *Alcatel-Lucent 5620 SAM Planning Guide* for more information about which ports need to be available.

3 The 5620 SAM-managed devices are configured to send SNMP packets of up to 9216 bytes. Check the MTU size, as described in Procedure 7-4.

Procedure 10-10 Problem: Cannot discover more than one device, or device resynchronization fails

Consider the following:

- When using SNMPv3 encryption, the engine ID of the managed device must be unique. As well, SNMP issues may result in Polling Problem alarms. Otherwise, the following issues may occur:
  - unreliable or slow discovery of network devices
  - resynchronization during scheduled polling fails
  - slow communication and synchronization times
  - polling fails completely
- When 5620 SAM resynchronizes some functions on a node, for example, BGP configurations for the 7750 SR, the SNMP packets may be broken into two or more smaller packets, when the maximum PDU size of 9126 bytes is exceeded.

When this happens for Release 2.0 and earlier versions of the 7750 SR with management access filter functionality enabled, the packets cannot be reassembled, and resynchronization fails.

- Each MIB entry policy has its own polling interval. When there is insufficient time in a polling interval for a resynchronization to occur, the interval may need to be changed to ensure proper resynchronization.

1 For resynchronization issues that may be caused due to insufficient MIB polling intervals.

2 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens with the General tab selected.

3 Ensure that the Polling Admin State is Up.

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

4 Check the MIB polling intervals for different managed devices, as required, by clicking on the MIB Entry Policies tab button. A list of MIBs appears, organized by managed device type.

i Select a MIB in the list and click on the Properties button.

ii Configure the Polling Interval parameter to ensure that sufficient time is configured for the polling to occur.

iii Configure the Administrative State of polling for the MIB entry, if required.

iv Click on the OK button to save the changes and close the form, or the Cancel button to close the form without saving changes, as required.

Procedure 10-11 Problem: Slow or failed resynchronization with network devices

When 5620 SAM performance is slow, especially when performing network device resynchronizations, SNMP and IP performance along the in-band or out-of-band interfaces between the network device and the 5620 SAM server may be the problem. Check the following:

- configuration of the LAN switch port and the 5620 SAM PC or workstation port match
- configuration of the LAN switch port and the network device management ports match
- mediation policy SNMP timeout and retry values are sufficient to allow the transfer of data between network devices and the 5620 SAM

1 Ensure that port configurations are compatible for the 5620 SAM server, the network device management ports, and the LAN switch. This is normally done by configuring auto-negotiation between the platforms, but your network may require more specific configuration.

2 Check whether all data is being transferred between the network device in-band management port and the 5620 SAM server.

i Open a Telnet or SSH session to the device from the 5620 SAM.

ii Check statistics on the in-band management port of the device:

```
# monitor port 1/2/3
```

Check the output for the following.

- errors that may indicate a communication problem with the a LAN switch.
- Over each time interval, is the number of input and output packets constant? This may indicate intermittent traffic.
- Are there more input packets or octets being transferred than output packets or octets? This may indicate a unidirectional traffic problem.

The types of error messages displayed determine the action to take.

- For failure errors, consider increasing the SNMP timeout value
- For collision errors, consider increasing the SNMP retry value

iii Check the mediation policy for the device using the 5620 SAM client GUI. Check the SNMP timeout and retry value for the mediation policy.

If the output of step ii indicates failures, consider increasing the default SNMP timeout value and perform step ii again.

When the output of step ii indicates frequent collisions, consider increasing the default SNMP number of retries value, then retest to see if resynchronizations are more reliable. Increasing the number of retries increases the likelihood that an SNMP packet is not dropped due to collisions.

You can check SNMP timeout and retry values from the Administration→Mediation menu. Click on the Mediation Security tab button.

Caution — When LAN performance is poor, increasing timeout values may mask an underlying problem. Increasing the SNMP timeout value in an environment where collisions are frequent reduces performance. Timeout values should be based on typical network response times

Check LAN communication issues, as specified in chapter 7. If problems persist, collect log information as specified in Procedure 2-1 and contact your Alcatel-Lucent support representative.

Procedure 10-12 Problem: Statistics are rolling over too quickly

Statistics database tables roll over, or lose statistics during an interval, if the tables fill before all statistics are collected or the next collection interval starts. To ensure sufficient statistics collection, consider the following:

- the statistics table size, depending on the configuration specified in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*
- the number of statistics collected, the number of objects with statistics collection enabled, and the frequency of statistics collection, as specified in the *5620 SAM User Guide*
- the OSS application requests data from the statistics tables less frequently than the configured roll over interval
- FTP must be enabled on the managed device in order for the 5620 SAM to retrieve statistics.

Alcatel-Lucent recommends that statistics collection planning includes the following considerations to prevent the loss of statistics data.

- measure the rate of statistics collection over a sufficient time interval
- determine the appropriate collection interval and statistics database table size based on individual network configurations
- ensure that the polling interval is sufficient for polled statistics

Procedure 10-13 Problem: Unable to receive alarms on the 5620 NM from the 5620 SAM

Check that the 5620 NM AS tool is properly configured to receive 5620 SAM alarms.

1 Ensure that the integration software is properly configured, as described in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

2 Configure the param.cfg file on the 5620 NM to ensure that alarms are forwarded from the 5620 SAM to the 5620 NM AS tool:

3 Open a command tool on the 5620 NM.

4 Navigate to the AS IM directory on the 5620 NM by typing:

/opt/netmgt/ALMAP/as/data/ascurim_0 ↵

5 Open the param.cfg file.

6 Set the NSP_USE_NSP parameter to True.

7 Ensure that the following param.cfg file parameters are configured to True:

- DROP_FREE_ALARMS
- CORBA_SERVER_DISCOVERY
- UNMANAGE_ON_TERMINATION

8 Save the changes and close the file.

11 — Troubleshooting the 5620 SAM database

11.1 Database troubleshooting

The following procedures describe how to troubleshoot 5620 SAM database issues.

Procedure 11-1 Problem: Database corruption or failure

You can restore a 5620 SAM database using a backup copy.

Note — Before you perform a database restore operation, you must shut down the databases and main servers in the 5620 SAM system. Contact Alcatel-Lucent technical support before you attempt to perform a database restore.

In a redundant 5620 SAM system, you must perform one or both of the following to regain database function and redundancy:

- Restore the primary database.
- Reinstantiate the standby database.

Both operations are required after a primary database failure. After a standby database failure, no restore operation is required, but you must reinstantiate the standby database to restore redundancy. You can use the 5620 SAM client GUI or a CLI script to reinstantiate a database.

Note 1 — In a redundant 5620 SAM system, you can restore a database backup only on a primary database station. To restore a database backup on a station other than the primary station, you must do the following on the station before you attempt the restore:

- Uninstall the 5620 SAM database, if it is installed.
- Install a primary database on the station.

Note 2 — In a redundant 5620 SAM system, you can reinstantiate a database only on a standby database station. To reinstantiate a database on a station other than the standby station, you must do the following on the station before you attempt the reinstantiation:

- Uninstall the 5620 SAM database, if it is installed.
- Install a standby database on the station.

See the *5620 SAM Maintenance Guide* for information about restoring a 5620 SAM database. See the 5620 SAM system redundancy chapter of the *5620 SAM User Guide* for information about 5620 SAM database reinstantiation.

Procedure 11-2 Problem: The database is running out of disk space

Sufficient database disk space is essential for efficient 5620 SAM database operation. You can also check whether your database backup schedule is adequate. Underscheduling backups while the database is in ARCHIVELOG mode creates numerous log files.

1. Verify that the database platform is adequately sized. The minimum platform requirements are available in the appropriate release notice or the *5620 SAM Planning Guide*, available from your Alcatel-Lucent technical-support representative.

2. Verify that the thresholds for disk space and archive logs are sufficient for your network, and determine how the disk space is being used. Contact your Alcatel-Lucent technical-support representative for more information.

3. Check the root database backup directory or partition to ensure that:

   - the size of the assigned disk space or slice is sufficient
   - the disk directory or slice is sufficient to hold the configured number of database backups

4. If the disk directory has many archived log files due to underscheduling of database backups, contact your Alcatel-Lucent technical-support representative for information about deleting archived log files.

5. Perform a database backup using the 5620 SAM client GUI or the 5620 SAM database configuration utility, as described in the *5620 SAM User Guide*.

6. Store the database backup in a secure location.

Procedure 11-3 Problem: A short database backup interval is creating database performance issues

Overscheduling the number of database backups may affect database performance, as the PC or workstation uses system resources to create the backups.

1. On a 5620 SAM client GUI, choose Administration→Database from the 5620 SAM main menu. The Database Manager form appears.

2. Click on the Backup tab button.

3. Check the Backup Interval and Interval Unit parameters. For example, setting the Backup Interval parameter to 6 and setting the Interval Unit parameter to hour means a backup is performed every 6 hours, or four times a day.

   This can cause performance issues, as database PC or workstation resources are used to create backups rather than to process requests.

4 Modify other parameters as required to improve performance.

5 Move the database backups to a secure location for storage or future use, according to your company policy.

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

Procedure 11-4 Problem: A database restore fails and generates a No backup sets error

Warning — Performing database modifications using Oracle database tools can cause irreparable harm to the database and your network management data, and can void your Alcatel-Lucent warranty or support agreement. Contact your Alcatel-Lucent technical-support representative for assistance with database troubleshooting.

Database backup sets expire based on a retention period. The default retention period is 365 days. After the retention period passes, the database backup sets are set to expired. You cannot restore databases from expired backup sets.

Contact your Alcatel-Lucent technical-support representative for more information about restoring a database.

Procedure 11-5 Problem: Database redundancy failure

Warning — Performing database modifications using Oracle database tools can cause irreparable harm to the database and your network management data, and can void your Alcatel-Lucent warranty or support agreement. Contact your Alcatel-Lucent technical-support representative for assistance with database troubleshooting.

Database redundancy between a primary database and a standby database is performed during installation on a Solaris workstation.

1 Ensure that the database redundancy configuration was performed properly, as specified in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*:

- The primary database is configured before the standby database.
- The primary and standby databases are on different workstations.
- The active and standby database directory structures and configurations are identical on both workstations.
- The same OS version and 5620 SAM software version is installed on the active and standby database workstations.

2 Ensure that there are no LAN communication problems between the active and standby database platforms. Consult your LAN troubleshooting guidelines or chapter 7 for more information.

Procedure 11-6 Problem: Primary or standby database is down

The status bar of the 5620 SAM client GUI indicates that the primary or standby database is down.

Warning — Performing database modifications using Oracle database tools can cause irreparable harm to the database and your network management data, and can void your Alcatel-Lucent warranty or support agreement. Contact your Alcatel-Lucent technical-support representative for assistance with database troubleshooting.

1 Verify the correct IP address and instance name of the database. From the 5620 SAM main menu, select Administration→Database to open the Database Manager. Verify the information in the Instance Name and DB Server fields.

2 Verify the network connectivity between the 5620 SAM primary server and the primary or standby database by ensuring that the primary server and the primary or standby database can ping each other. See chapter 7 for more information.

Procedure 11-7 Problem: Need to verify that Oracle database and listener services are started

Perform the following procedure to determine the status of the Oracle database and listener services, each of which starts automatically during system initialization.

1 Open a 5620 SAM GUI client.

2 View the status bar at the bottom of the GUI. The background of the database section of the status bar is yellow or red when there is a problem with a database service. The status bar text indicates the database service status.

3 If the database is on a Windows station, perform the following steps to ensure that automatic startup is enabled for the Oracle database and listener services.

i Log in to the database station as a local administrator.

ii Choose Start→Settings→Control Panel→Administrative Tools→Services.

iii Scroll through the list of services and verify that the OracleTNSListener and OracleService*database_name* services each show a Startup Type of Automatic.

iv If the Startup Type of a service is not Automatic, perform the following steps.

- Right-click on the service name and choose Properties from the contextual menu. The *service_name* Properties form opens.
- Choose Automatic from the Startup type drop-down list.
- Close the *service_name* Properties form.
- Close the Services form.
- Close Control Panel.

Procedure 11-8 Problem: Need to determine status or version of database or Oracle proxy

Perform the following procedure to determine the status of the database or Oracle proxy, each of which starts automatically during system initialization.

1 Log in as the appropriate user on the database station. For Solaris, you must log in as the oracle management user. For Windows, you must log in as a local administrator.

2 Open a console window on the database station.

3 Navigate to the *installation_directory*/install/config/samdb directory

where *installation_directory* is the database installation location, typically /opt/5620sam/samdb on Solaris or C:\5620sam\samdb on Windows

4 Enter the following command.

```
oracleproxy.ext option ↵
```

where
ext is sh for Solaris, or bat for Windows
option is one of the options in Table 11-1

Table 11-1 oracleproxy.* flag options

Flag option	Description
start	Starts the 5620 SAM Oracle proxy
no option, or help	Lists the available options
proxy_version	Displays Oracle proxy version information
proxy_status	Displays Oracle proxy status information
db_version	Displays 5620 SAM database version information
db_status	Displays 5620 SAM database status information

5 Review the command output.

The following sample shows the output of the proxy_status option.

```
Proxy is UP
```

The following sample shows the output of the db_version option.

```
5620 SAM Version 8.0 R1 - Built on Wed Apr 21 03:14:15 EST 2010
```

6 Close the console window.

12 — 5620 SAM client GUI warning message output

12.1 5620 SAM client GUI warning message overview

Warning messages in the 5620 SAM client GUI provide an error recovery mechanism to inform you when:

- information has been entered incorrectly
- additional information is required
- the operation you are attempting cannot be completed
- a change to a configuration sub-form is not committed until the parent form is committed
- an operation that may result in service disruption is requested
- a configuration form for an object is open that can potentially conflict with a previously opened form

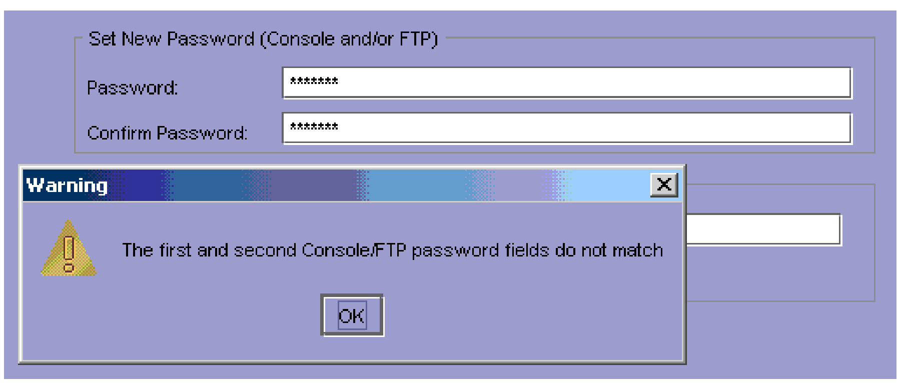
When an error condition is encountered that the 5620 SAM client has not anticipated, a Problems Encountered window is displayed. See section 13.1 for more information.

You can use the client GUI to suppress warning messages within containing windows. See the *5620 SAM User Guide* for more information.

Incorrect data entry

When incorrect information is entered for a parameter, a warning message that describes the error is displayed. For example, when you configure a password for a site user, the value entered for the Password parameter and the Confirm Password parameter must match. If they do not match, a warning message is displayed, as shown in Figure 12-1.

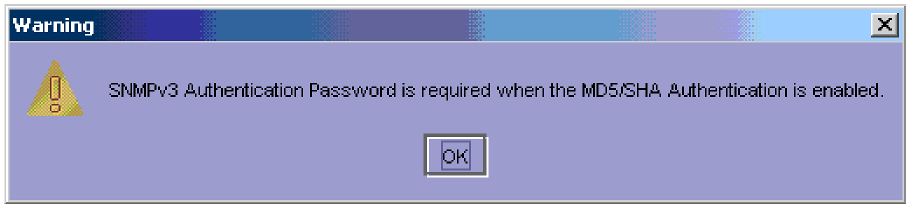
Figure 12-1 Password mismatch warning dialog box



Additional information required

When the value selected for a parameter has a that requires another parameter to be configured, a warning message indicates the missing information that is required. For example, when you configure a new or existing user with MD5 or SHA as the value for the Authentication Protocol parameter, a password must be configured. If you do not configure a password, a warning message is displayed, as shown in Figure 12-2.

Figure 12-2 Password missing warning dialog box



The warning message indicates the information that is required. In this case, click on the OK button to close the dialog box, and configure the New Authentication Password and Confirm New Auth Password parameters.

Unable to complete requested action

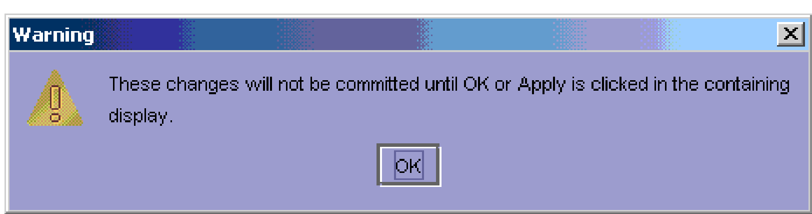
Warning messages are used to indicate that a specific action cannot be completed. These warnings may occur when you try to create a new object or modify an existing object that results in an unsupported configuration. For example, the message "Can't bind LSP to a non-mpls service tunnel" indicates that you cannot bind an LSP to a service tunnel that is not configured with the MPLS protocol.

These errors can be difficult to resolve and may require that you retrace your steps to determine the cause of the warning. Check the documentation to ensure that you are following procedures correctly.

Commitment of changes from a form and its sub-forms

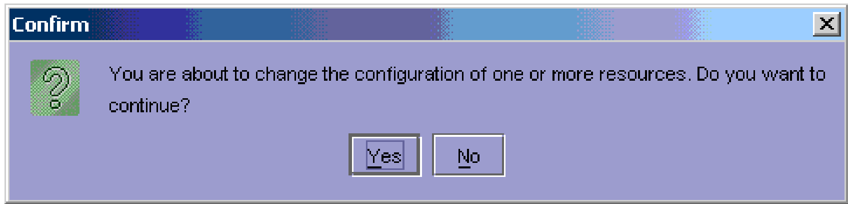
From a configuration form, you can open sub-forms that require completion before you continue with the parent form. For example, when you create a VLL service, the Create Service Site form opens during one of the configuration steps. After you configure parameters in this sub-form and click on the Finish button, a warning message is displayed, as shown in Figure 12-3.

Figure 12-3 Committing changes warning dialog box



Changes entered in the sub-form are not committed until you click on the OK or Apply button of the parent form. When you click on the OK or Apply button of the parent form, a final confirmation is displayed, as shown in Figure 12-4.

Figure 12-4 Committing changes to resources warning dialog box

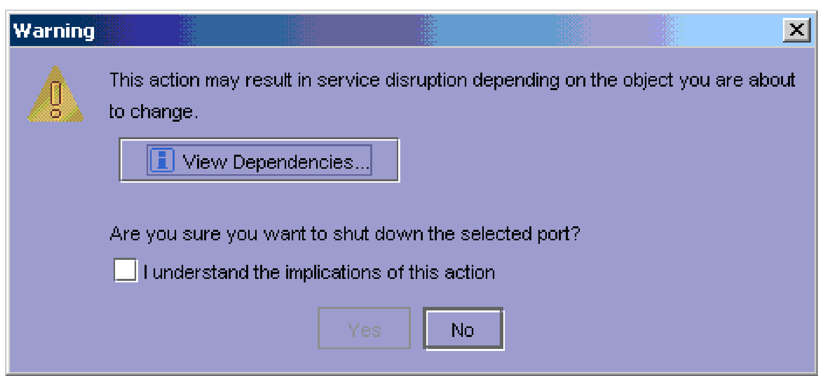


When you click on the Yes button for the last confirmation the changes to the parent or sub-forms are committed.

Service disruption warning

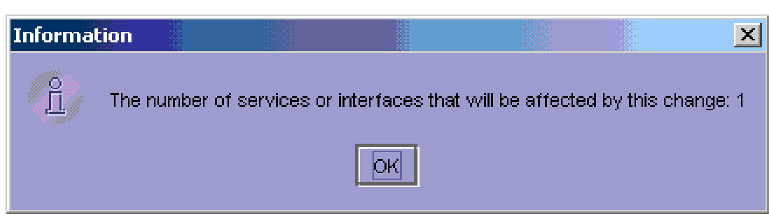
A service disruption dialog box is displayed when you perform an action that may be service-affecting. For example, if you attempt to shut down a daughter card, a warning message is displayed, as shown in Figure 12-5.

Figure 12-5 Service disruption warning dialog box



As indicated by the warning message, the action you are about to perform may cause a disruption to customer service because of a potential dependency that another object or service has on the current object. Click on the View Dependencies button to indicate the number of services that may be affected by the action, as shown in Figure 12-6.

Figure 12-6 View dependencies warning dialog box

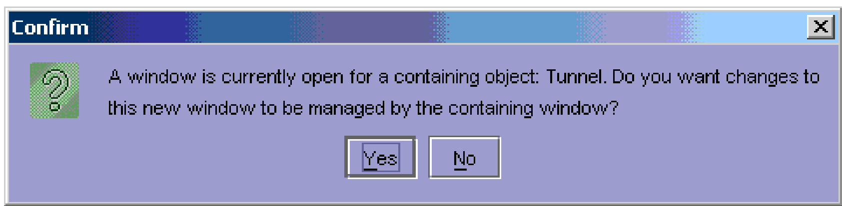


Verify that the requested action is appropriate. Click on the checkbox beside the statement “I understand the implications of this action” to continue with the action.

Duplicate configuration form conflicts

There are multiple ways to access a configuration form for the same object. For example, you can view the configuration form for a port by choosing Manage→Equipment, or you can access the port from the Application→Equipment Window form. When you try to perform both accesses, a warning message is displayed, as shown in Figure 12-7.

Figure 12-7 Duplicate form warning dialog box



When this warning message is displayed, another form is open for the same object. When two forms are open concurrently for the same object, there may be unexpected results because changes committed from one form are not reflected in the other form.

12.2 Responding to 5620 SAM client GUI warning messages

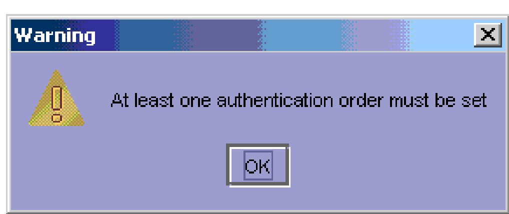
The following procedure describes how to respond to a warning message when you perform an action with the 5620 SAM client.

Procedure 12-1 To respond to a warning message

1 Perform an action.

A warning message dialog box opens. For example, when you configure a site password policy, at least one authentication order must be specified as the default in order to configure the authentication order parameters. If at least one authentication order is not configured, a warning message is displayed, as shown in Figure 12-8.

Figure 12-8 Authentication warning dialog box



2 After you read the warning message, click on the OK button. The warning message dialog box closes.

3 Correct the problem based on the information provided. For the example in Figure 12-8, configure the authentication order parameters.

4 If you cannot correct the problem and continue to get the same warning message:

a Check the documentation to ensure that you are following the steps correctly.

b Verify that you are trying to perform an action that is supported.

c Review the general troubleshooting information in section 1.3.

d If you cannot resolve the problem, perform Procedure 2-1 before you contact your technical support representative.

13 — Troubleshooting with Problems Encountered forms

13.1 Problems Encountered form overview

The Problems Encountered form reports error conditions on the client software for which there are no associated warning messages or when the client software cannot identify the problem. Figure 13-1 shows the Problems Encountered form.

Figure 13-1 Problems Encountered form

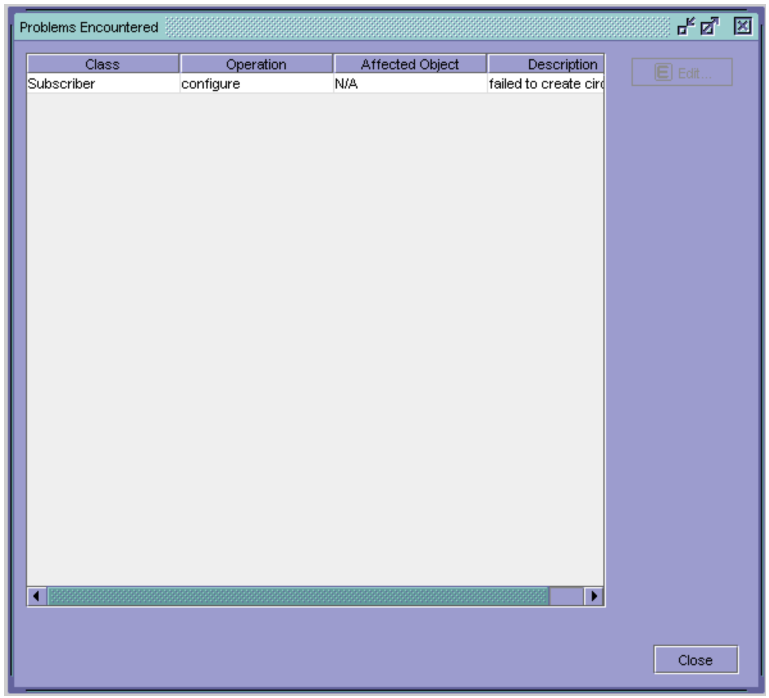


Table 13-1 describes the fields in the Problems Encountered form.

Table 13-1 Problems Encountered form field descriptions

Field name	Description
Class	Specifies the object type that is the source of the problem
Operation	Specifies the type of operation that was attempted when the problem occurred.
Affected Object	Specifies the name of the affected object. Typically, if a Problems Encountered form appears when you are trying to create a object, this field contains N/A because the object has not been created.
Description	Specifies a short description of the problem, which may help you determine the cause of the problem and how to correct the problem. For additional information, click on the Properties button. The information may not be enough for you to correct the problem. The information can be used by your technical support representative to help resolve the problem.

13.2 Using Problems Encountered forms

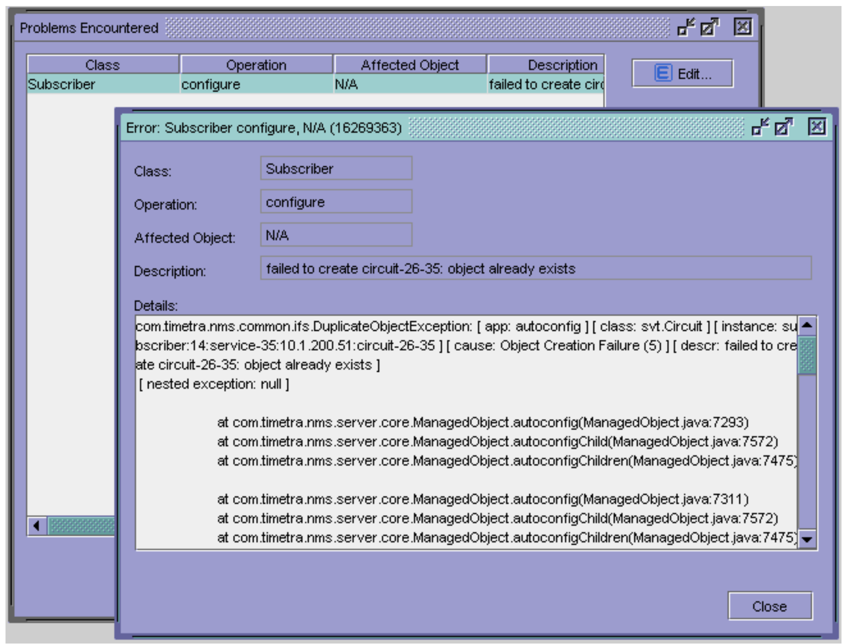
The following procedures describe how to view additional information about a problem in a Problems Encountered form and the information to collect before you contact your technical support representative.

Procedure 13-1 To view additional problem information

1 Choose an entry in the Problems Encountered form.

2 Click on the Properties button. Figure 13-2 shows a form with the problem details.

Figure 13-2 Problems Encountered form details



3 Try to correct the problem based on the information provided. If you cannot correct the problem, complete the procedure and perform Procedure 13-2.

4 Click on the Close button to close the details window.

5 If there is more than one problem, repeat steps 2 to 4.

6 Click on the Close button.

Procedure 13-2 To collect problem information for technical support

The following procedure describes what to do before you contact your technical support representative when you cannot resolve a problem on the Problems Encountered form.

1 Review the problem information in the Problems Encountered form, as described in Procedure 13-1.

2 Record the actions performed up to the point when the Problems Encountered form appeared. For example, if you were trying to create a VLL service, record the details about the service that you were trying to create.

3 Record the appropriate problem information, as described in section 1.3.

4 Collect logs for your Alcatel-Lucent support representative, as described in Procedure 2-1.

14 — Troubleshooting with the client activity log

14.1 The 5620 SAM Usage and Activity Records overview

The 5620 SAM Usage and Activity Records form allows users with administrative privileges to view user activity for 5620 SAM GUI and OSS clients. Figure 14-1 shows the 5620 SAM Usage and Activity Records form.

Figure 14-1 5620 SAM Usage and Activity Records form details

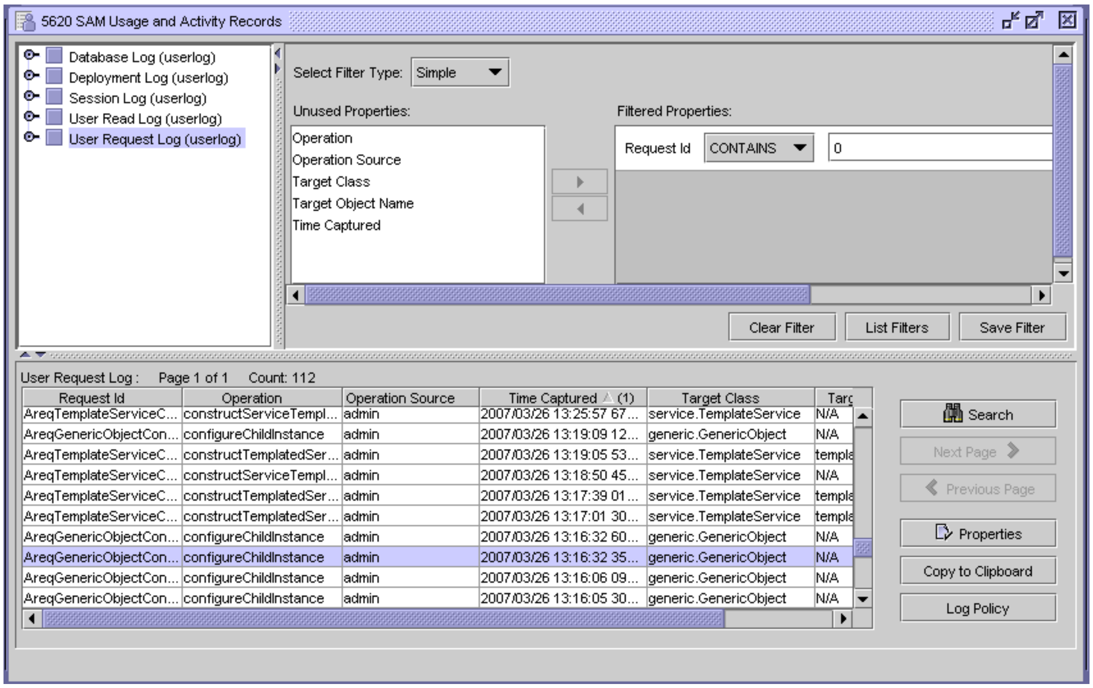


Table 14-1 describes the types of logs available in the 5620 SAM Usage and Activity Records form.

Table 14-1 Log types available in the 5620 SAM Usage and Activity Records form

Log name	Description
Database Log	To view information about changes to the database
Deployment Log	To view information about deployment requests sent from the client GUI and OSS
Session Log	To view information about clients connecting and disconnection from the client GUI and OSS, including security failures
User Read Log	To view information about data viewed by users from the client GUI and OSS
User Request Log	To view information about user requests sent from the client GUI and OSS

The 5620 SAM database stores the log records associated with the user activity. A system administrator can use the 5620 SAM-O interface to export log data in an XML format. (Filtered lists of log entries can also be retrieved through the 5620 SAM-O interface.) You can use the XML log data as an archive mechanism or statistical analysis method. See the *5620 SAM-O OSS Interface Developer Guide* for more information.

The 5620 SAM GUI allows administrative operators to view client activity log entries. The default setting of the 5620 SAM is to chronologically sort the log entries. You can also filter a log based on the following criteria:

- user who initiated the operation
- request ID associated with the operation
- operation type
- operation source
- result for the operation
- object that was the target of the operation
- execution status of the operation
- read-write requests from OSS interfaces

Note — You must manually refresh the display in the 5620 SAM Usage and Activity Records form to view latest log entry information.

There can be multiple log entries for a single client operation, for example:

- request received
- database update
- deployment

You can use the request ID for log entries to:

- correlate the log entries associated with a single client operation
- sort the client activity log and identify the log entries associated with a single client operation

There may be no log entries associated with a particular client operation.

Table 14-2 lists the log file entries for some 5620 SAM client activities. Logging is enabled by default in the 5620 SAM.

Table 14-2 Log file information

Action	Log file entries
Receive client request	• date and time the log entry was created • user who initiated the request • request ID (supplied by the client) • package-qualified class of the target object • fully distinguished name of the target object • name of the target object (if different from the fully distinguished name • name of the operation requested • source of the request (GUI or XML OSS interface)
Completion of database update	• date and time the log entry was created • user who initiated the request • request ID (supplied by the client) • type of operation performed (insert, delete, or modify) • fully distinguished name of the target object • result of the update (success or failure)
Completion of deployment operation	• date and time the log entry was created • user who initiated the request • request ID (supplied by the client) • deployer ID • deployment stage • package-qualified class of the target object • fully distinguished name of the target object • result of the deployment (success or failure)
Failed authentication attempt, either through native 5620 SAM authentication or through an external authentication mechanism [1]	• date and time the log entry was created • name of the operator the event relates to • type of event, for example, failed login or disabled account
Disabling of a user account because of too many failed authentication attempts [1]	
Violation of user permissions through the XML OSS interface [1]	

Note

[1] The 5620 SAM also raises an alarm for log entries that are related to security.

14.2 Using the 5620 SAM Usage and Activity Records forms

The following procedures describe how to use the 5620 SAM Usage and Activity Records form to correlate user requests and deployment activity.

Procedure 14-1 To identify the user associated with a network problem

1 Choose Administration→Security→5620 SAM Usage and Activity Records from the 5620 SAM main menu. The 5620 SAM Usage and Activity Records form opens.

2 Select Deployment Log (userlog) in the upper left panel as the search criterion.

3 Select the filter criteria for the log display, if required.

4 Click on the Search button. A list of deployment log activity appears.

5 Identify the network problem by reviewing the status of the Result column. There is no check mark in the Result column for a failed deployment.

6 Identify and record the request ID for the failed deployment using the Request Id column.

7 Click on User Request Log (userlog) on the 5620 SAM Usage and Activity Records form.

8 Use the filter in the User Request Log (userlog) to list the requests for the request ID that you obtained in step 6. The 5620 SAM displays the filter results in the Userlog display area. The Operation Source column identifies the user associated with the failed deployment.

Procedure 14-2 To identify the database activity for a user request

1 Choose Administration→Security→5620 SAM Usage and Activity Records from the 5620 SAM main menu. The 5620 SAM Usage and Activity Records form opens.

2 Click on User Request Log (userlog) on the 5620 SAM Usage and Activity Records form.

3 Select the filter criteria for the log display, if required.

4 Click on the Search button. A list of user request entries appears.

5 Identify and record the request ID for the user request using the Request Id column.

6 Click on Database Log (userlog) on the 5620 SAM Usage and Activity Records form.

7 Use the filter in the Database Log (userlog) to list the database activity associated with the request ID that you obtained in step 5. The 5620 SAM displays the filter results in the Userlog display area.

Procedure 14-3 To identify the deployment results for a user request

1. Choose Administration→Security→5620 SAM Usage and Activity Records from the 5620 SAM main menu. The 5620 SAM Usage and Activity Records form opens.
2. Select the filter criteria for the log display, if required.
3. Click on the Search button. A list of user request log activity appears.
4. Identify and record the request ID for the user request using the Request Id column.
5. Click on Deployment Log (userlog) on the 5620 SAM Usage and Activity Records form.
6. Use the filter in the Deployment Log (userlog) to list the deployment results associated with the request ID that you obtained in step 4. The 5620 SAM displays the search results.
7. Identify whether the user action resulted in a successful network deployment by reviewing the status of the Result column. There is no check mark in the Result column for a failed deployment.

Procedure 14-4 To retrieve historical user logs

Note — A user with LI privileges can view LI -related activity and usage records. A 5620 SAM user with the appropriate access privileges can view non-LI related activity and usage records.

1. Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM Usage and Activity Records from the 5620 SAM main menu. The 5620 SAM Usage and Activity Records form opens.
2. Choose a type of user log from the object drop-down list:
   - Database Log to view information about changes to the database due to actions performed by the client
   - Deployment Log to view information about deployment requests sent from the client
   - Session Log to view information about the current client session, including operations performed and permissions for the logged in user account
   - User Read Log to view information about data viewed by users of the client
   - User Request Log to view information about user requests sent from the client
3. Configure the list filter criteria and click on the Search button. A list of log records is displayed. You can sort the log records by clicking on a list column heading.
4. To view a log record, select the record and click on the Properties button. The Log Record form for the entry opens. The parameters and information displayed depends on the type of log.

5 When you are finished viewing the log record, click on the Close button. The Log Record form closes.

6 You can perform other functions, such as displaying a count of the records or saving the records to a file for post-processing purposes, by right-clicking on a column heading and choosing an option from the contextual menu.

7 Close the 5620 SAM Usage and Activity Records form.

Customer documentation and product support

Customer documentation

http://www.alcatel-lucent.com/myaccess

Product manuals and documentation updates are available at alcatel-lucent.com. If you are a new user and require access to this service, please contact your Alcatel-Lucent sales representative.

Technical Support

http://support.alcatel-lucent.com

Documentation feedback

documentation.feedback@alcatel-lucent.com

3HE 05723 AAAE TQZZA Edition 01