Alcatel-Lucent 5620

SERVICE AWARE MANAGER | RELEASE 5.0

TROUBLESHOOTING GUIDE

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

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.

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

About this document

The *5620 SAM Troubleshooting Guide* provides task-based procedures and user documentation to:

- collect data to help resolve issues in the network and network management domains
- 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

About related documentation

There are several documents that describe the 5620 SAM and the managed devices.

- See the *5620 SAM Planning Guide* for information about 5620 SAM scalability and recommended hardware configurations.
- See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about installing the 5620 SAM database, server, and client software.
- See the *5620 SAM User Guide* for information about using the client GUI to perform network management functions.
- See the *5620 SAM Parameter Guide* for definitions, ranges, dependencies, and default values for configurable 5620 SAM client GUI parameters.
- See the *5620 SAM-O OSS Interface Developer Guide* for information about using the XML OSS interface to create OSS applications, for example, to perform alarm monitoring and inventory control.
- See the *5620 SAM Routine Maintenance Procedures Guide* for information about developing and scheduling regular maintenance activities.
- See the *5620 SAM System Architecture Guide* for information about software component interaction.
- See the *5620 SAM NE Compatibility Guide* for release-specific information about the compatibility of managed-device features with different 5620 SAM releases.
- See the *5620 SAM Statistics Management Guide* for information about managing 5620 SAM statistics collection and to view a list of the MIB counters that are available for collection using the 5620 SAM.
- See the *5620 SAM CNM and OSS Toolkit Guide* for information about creating CNM applications.
- See the index file in the User_Documentation directory on the application DVD for additional documentation information.

See the 7750 SR, 7450 ESS, 7710 SR, 7250 SAS, and Telco user documentation for information about device-specific CLI commands, parameters, and installation. Contact your Alcatel-Lucent support representative for information about specific network or facility considerations.

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→User Documentation in the 5620 SAM client GUI main menu

Conventions used in this guide

Table 1 lists the conventions that are used throughout the 5620 SAM documentation. The conventions may not appear in all documents.

Table 1 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
↵	Press the Return key	↵
—	An em dash indicates there is no information.	—
→	Indicates that a cascading submenu results from selecting a menu item	Policies→Routing

Procedures with options or substeps

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

Example of options in a procedure

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

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

a This is one option.

b This is another option.

2 You must perform this step.

Example of substeps in a procedure

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

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

i This is the first substep.

ii This is the second substep.

iii This is the third substep.

2 You must perform this step.

Important information

The following conventions are used to indicate important information:

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 provides information that is, or may be, of special interest.

Contents

Network troubleshooting

Network management troubleshooting

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 Routine Maintenance Procedures 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 Routine Maintenance Procedures 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://www1.alcatel-lucent.com/profile/forms/login.jhtml 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/wps/portal/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, Linux, 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 EmsServerLog.txt file from the *install _directory* 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 — Troubleshooting using 5620 SAM

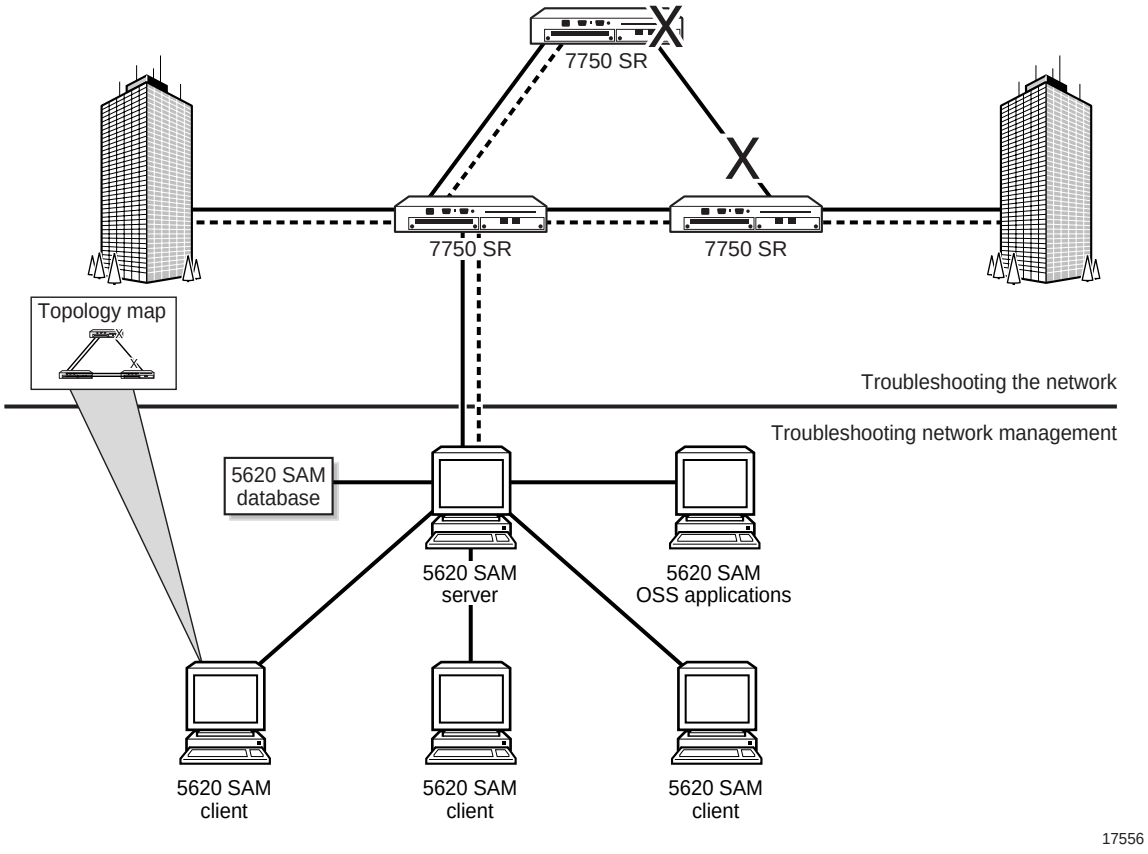
2.1 5620 SAM troubleshooting process

The *5620 SAM Troubleshooting Guide* is intended for NOC operations and other engineering operational staff who are responsible for identifying and resolving performance issues in 5620 SAM-managed IP/MPLS networks. This guide uses the following general categories for troubleshooting-related tasks:

- troubleshooting the network
- troubleshooting network management

Figure 2-1 shows the difference between the 5620 SAM troubleshooting categories.

Figure 2-1 5620 SAM troubleshooting categories



Troubleshooting the network

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

Alarms for network objects

The 5620 SAM converts SNMP traps from network devices to events and alarms. You can then use the 5620 SAM to correlate the events and alarms against the managed equipment, and the 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 form, and customer information form that lists the affected service.

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

Service problems with no associated alarms

The proper delivery of services requires a number of operations must occur correctly at different levels within the service creation model. For example, operations such as the association of packets to a service, VC labels to a service, and each service to a service tunnel 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, 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 the connection.

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 are kept within the service provider network and not forwarded to the customer. For out-of-band testing, OAM packets are sent across some portion of the transport network. For example, 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 network management

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, 5620 SAM-O servers, and 5620 SAM client software
- Windows, Solaris, and Linux operating systems
- PC and workstation platforms
- 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 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 "Service assurance OAM diagnostics for troubleshooting services" in section 4.1 for more information.

Event log and property files

You can use log and property files to help troubleshoot your network.

The number of log files generated can use large amounts of disk space if systems run for long periods with significant activity. Ensure that the contents of the various log directories are backed up on a regular basis. See the *5620 SAM Routine Maintenance Procedures Guide* for more information about how to perform routine maintenance on your network.

Note — The event log and property files can be overwritten or removed when you reboot a PC or workstation running 5620 SAM software.

Procedure 2-1 To collect troubleshooting logs and property files

1 Collect the following files for troubleshooting a 5620 SAM installation:

- stderr and stdout information displayed on the console
- log files from the /tmp directory with the title 5620*nameofapplication*.txt and from the *install_directory* with the title 5620*nameofapplication*.txt

2 If required, collect the following individual troubleshooting log files before you reboot or restart 5620 SAM software during troubleshooting:

a To troubleshoot a 5620 SAM database, collect the dbconfig.properties file from the *installation_directory*/config directory or folder. Also collect:

- alert_*database_instance*.log file from the *database_install_directory*/admin/*database_instance*/bdump directory
- OracleProxyLog.txt file from the *database_install_directory*/admin/*database_instance*/proxy directory

b To troubleshoot a 5620 SAM client, collect the nms-client.xml file from the *installation_directory*/nms/config directory or folder. Also collect the EmsClientLog.txt file from the *installation_directory*/nms/log directory or folder.

c To troubleshoot a 5620 SAM installation problem, collect the installation logs from the *installation_directory* and locate the 5620_SAM.install.*data*.txt files.

d Collect server and client logs, for example, the EmsServerLog or Clip_log for 7250 SAS and Telco CLE device management, from the *installation_directory*/nms/log directory or folder. After logs reach a certain size, usually 4 Mbytes, the data is put in an old log file and a new log file is started. There may be many log files in the directory or folder, depending on how long the 5620 SAM software has been running.

Note — Log files are generally overwritten when systems are restarted. Also, applications that run for long periods can generate multiple log files. Verify that there is sufficient disk space to store the log files. Most log files are stored in the *install_directory*/version/nms/log directory or folder.

3 If required, you can run the getSAMDebugFiles.bash utility on a Solaris stations to collect a comprehensive group of troubleshooting log files for use by Alcatel-Lucent technical support to troubleshoot a problem.

i Open a command or shell tool on the 5620 SAM server.

ii Navigate to the *installation_directory*/nms/bin directory.

iii Run:

```
getSAMDebugFiles.bash ↵
```

iv Copy the getSAMDebugFiles.bash utility to the 5620 SAM database *installation_directory*/nms/bin directory.

v Run:

```
getSAMDebugFiles.bash ↵
```

vi Collect the output of the utility tool.

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

vii Send the files to support when requested.

4 Store the files in a secure location until they are sent to support, and ensure that the files are not overwritten. For example, if there are two 5620 SAM clients with troubleshooting issues, rename the files, as appropriate, to identify each 5620 SAM client and to prevent overwriting of one file with another of the same name.

2.3 Workflow to troubleshoot your network using 5620 SAM

The following workflow correlates the tasks in the *5620 SAM Network Management Troubleshooting Guide* with the problem-solving model described in section 1.2.

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

2 Categorize the problem. Table 2-1 describes the general categories that are associated with troubleshooting 5620 SAM.

Table 2-1 5620 SAM general troubleshooting categories

Category	Category description
Network problem	A 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 to view network health
Network management problem	A domain, connectivity, platform-related, or configuration problem Network management domain and LAN troubleshooting Solaris and Linux platform troubleshooting PC operating system issues GUI and OSS client 5620 SAM software issues 5620 SAM and 5620 SAM-O server software issues 5620 SAM database and Oracle software issues Warning messages related to configuration issues Problems Encountered form detailing programming exceptions Activity log forms detailing user, database, and deployment history

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

a For a network problem, see:

i General Procedure 3.2 for specific information about the workflow to investigate and resolve alarm conditions on a network object or customer service.

ii General Procedure 4.2 for specific information about the workflow to detect and resolve problems on customer services with no associated alarms.

Note — Chapter 5 contains general information about the surveillance and troubleshooting of a managed network. There are no sub-level workflows for the topics in this chapter.

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

Table 2-2 5620 SAM network management problems

Problem	Solution
Troubleshooting network management LAN problems	
Problem: All network management domain PCs and workstations are experiencing performance degradation	Procedure 6-1
Problem: Lost connectivity to one or more network management domain PCs or workstations	Procedure 6-2
Problem: Another machine can be pinged, but some functions are unavailable	Procedure 6-3
Problem: packet size and fragmentation issues	Procedure 6-4
Troubleshooting Solaris and Windows platforms	
Problem: Slow processing on a Solaris workstation and CPU peaks	Procedure 7-1
Problem: Slow performance on a Solaris workstation, but no spike or peak in the CPU	Procedure 7-2
Problem: There is excess disk activity on my Solaris platform	Procedure 7-3
Problem: There is not enough swap space added or the Solaris platform is disk bound	Procedure 7-4
General information about troubleshooting the Windows platform	Section 7.2
Troubleshooting 5620 SAM client GUIs and client OSS applications	
Problem: Delayed server response to client activity	Procedure 8-1
Problem: Unable to print from Solaris platform client	Procedure 8-2
Problem: Cannot place newly discovered device in managed state	Procedure 8-3
Problem: I performed an action, such as saving a configuration, but I cannot see any results	Procedure 8-4
Problem: Device configuration backup not occurring	Procedure 8-5
Problem: 5620 SAM client unable to communicate with 5620 SAM server	Procedure 8-6
Problem: Cannot start 5620 SAM client, or error message during client startup	Procedure 8-7
Problem: Cannot view 5620 SAM alarms using 5620 NM client	Procedure 8-8

(1 of 3)

Problem	Solution
Problem: 5620 SAM client GUI shuts down regularly	Procedure 8-9
Problem: Configuration change not displayed on 5620 SAM client GUI	Procedure 8-10
Problem: List or search function takes too long to complete	Procedure 8-11
Problem: Cannot select certain menu options or cannot save certain configurations	Procedure 8-12
Problem: Cannot clear alarms using 5620 SAM client GUI	Procedure 8-13
Problem: Exception error message about untrusted SSL PKI certificate	Procedure 8-14
Problem: Cannot open user documentation from 5620 SAM client GUI	Procedure 8-15
Troubleshooting 5620 SAM server issues	
Problem: Cannot manage new routers or cannot start the 5620 SAM main server	Procedure 9-1
Problem: A 5620 SAM server on a Solaris platform cannot be reached or does not respond	Procedure 9-2
Problem: Excessive 5620 SAM server response time	Procedure 9-3
Problem: Unsure of the status of a 5620 SAM main or auxiliary server	Procedure 9-4
Problem: All SNMP traps from managed devices are arriving at one 5620 SAM server, or no SNMP traps are arriving	Procedure 9-5
Problem: Cannot discover more than one device or a resynchronization of devices fails	Procedure 9-6
Problem: A 5620 SAM server starts up, and then quickly shuts down	Procedure 9-7
Problem: Unable to receive alarms on the 5620 NM from the 5620 SAM	Procedure 9-8
Problem: Unable to receive alarms on the 5620 SAM, or alarm performance is degraded	Procedure 9-9
Problem: Communication issues between a 5620 SAM server and database	Procedure 9-10
Problem: Statistics are rolling over too quickly	Procedure 9-11
Problem: Server is unresponsive after SSL is configured	Procedure 9-12
Problem: Slow or failed resynchronization with network devices	Procedure 9-13
Problem: The 5620 SAM server startup does not respond while trying to connect to database sessions	Procedure 9-14
Troubleshooting the 5620 SAM database	
Problem: My database is running out of disk space	Procedure 10-1
Problem: A short database backup interval is creating database performance issues	Procedure 10-2
Problem: I need to immediately restore a backed-up database to recover from a catastrophic problem	Procedure 10-3
Problem: I need to restore a database	Procedure 10-4
Problem: The database restore fails with a no backupsets error	Procedure 10-5
Problem: Database redundancy is not working	Procedure 10-6
Problem: Primary or standby database is down	Procedure 10-7
Problem: Unable to verify that Oracle database and listener services are started	Procedure 10-8
Problem: Unable to verify status or version of the database or Oracle proxy	Procedure 10-9
Troubleshoot using the GUI warning messages	

(2 of 3)

Problem	Solution
To respond to a warning message	Procedure 11-1
Troubleshoot with Problem Encountered forms	
To view additional problem information	Procedure 12-1
To collect problem information for technical support	Procedure 12-2
Troubleshoot with the client activity log	
To identify the user associated with a network problem	Procedure 13-1
To identify the database activity for a user request	Procedure 13-2
To identify the deployment results for a user request	Procedure 13-3
To retrieve historical user logs	Procedure 13-4

(3 of 3)

4 Verify the solution.

Network troubleshooting

3 — Troubleshooting network alarms

3.1 Troubleshooting using network alarms strategy

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 generated by 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

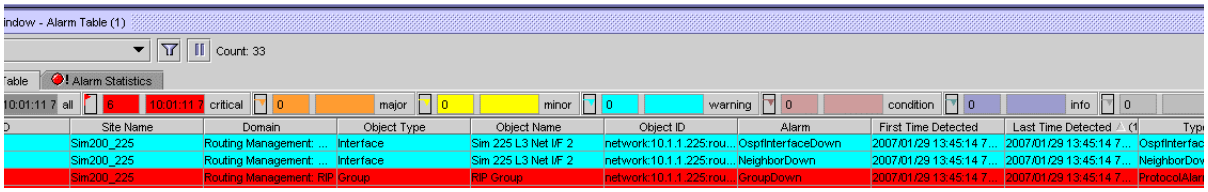
Use the following procedures to troubleshoot network problems using alarms.

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 generated.

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



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

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 generated at the same time, use the alarm information provided to determine which alarm may be closer to the root cause of the problem and start troubleshooting with 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 network managed objects

Level	Managed object	Alarm domain (domain descriptor)	For alarm information see
—	General network-management or 5620 SAM-related objects	Anti-spoofing (antispoof)	Table 3-2
		APS (aps)	Table 3-3
		CCAG (ccag)	Table 3-6
		Circuit emulation (circem)	Table 3-7
		Database (db)	Table 3-8
		File policy (file)	Table 3-11
		Generic object (generic)	Table 3-12
		L2 (layer2)	Table 3-20
		L2 forwarding (l2fwd)	Table 3-17
		L3 forwarding (l3fwd)	Table 3-18
		LAG (lag)	Table 3-19
		Mediation (mediation)	Table 3-10
		MSDP (msdp)	Table 3-26
		NE security (sitesec)	Table 3-43
		Policy (policy)	Table 3-30
		PPP (ppp)	Table 3-31
		RADIUS accounting (radiusaccounting)	Table 3-32
		Residential subscriber (ressubscr)	Table 3-33
		Scheduler (vs)	Table 3-57
		Security (security)	Table 3-40
		Server (server)	Table 3-41
		Software (sw)	Table 3-48
		STM (sas)	Table 3-39
		Subscriber identification (subscrident)	Table 3-46
		Template (template)	Table 3-50
		VRRP (vrrp)	Table 3-56
1	Network	Network (netw)	Table 3-27
		NE (rtr)	Table 3-37
		Monitored path (monpath)	Table 3-24
		SRRP (srrp)	Table 3-45
2	Service	I-pipe (ipipe)	Table 3-15
		Service management (service)	Table 3-42
		Service mirror (mirror)	Table 3-23
		VLANs (vlan)	Table 3-53
		VLL (vll)	Table 3-54
		VPLSs (vpls)	Table 3-55
3	SDP binding	Service tunnel management (tunnelmgmt)	Table 3-52
4	Tunnel	MPLS (mpls)	Table 3-25
		Rules (rules)	Table 3-38
		Service tunnel (svt)	Table 3-47
		Topology (topology)	Table 3-51
5	LSP binding	MPLS (mpls)	Table 3-25
6	LSP		
7	Session	RSVP (rsvp)	Table 3-36

(1 of 2)

Level	Managed object	Alarm domain (domain descriptor)	For alarm information see
8	LDP interface or targeted peer	LDP (ldp)	Table 3-21
9	Interface or network interface	BGP (bgp) IGMP (igmp) IS-IS (isis) OSPF (ospf) PIM (pim) RIP (rip)	Table 3-4 Table 3-14 Table 3-16 Table 3-28 Table 3-29 Table 3-34
10	Physical equipment	Equipment (equipment) Ethernet equipment (ethernetequipment) Generic Network Element (genericne) RMON (rmon)	Table 3-9 Table 3-9 Table 3-13 Table 3-35
11	SONET / SDH bundle SONET port/channel	Bundle (bundle) SONET equipment (sonetequipment)	Table 3-5 Table 3-44
12	DS1 / E1 channel	TDM equipment (tdmequipment)	Table 3-49

(2 of 2)

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.

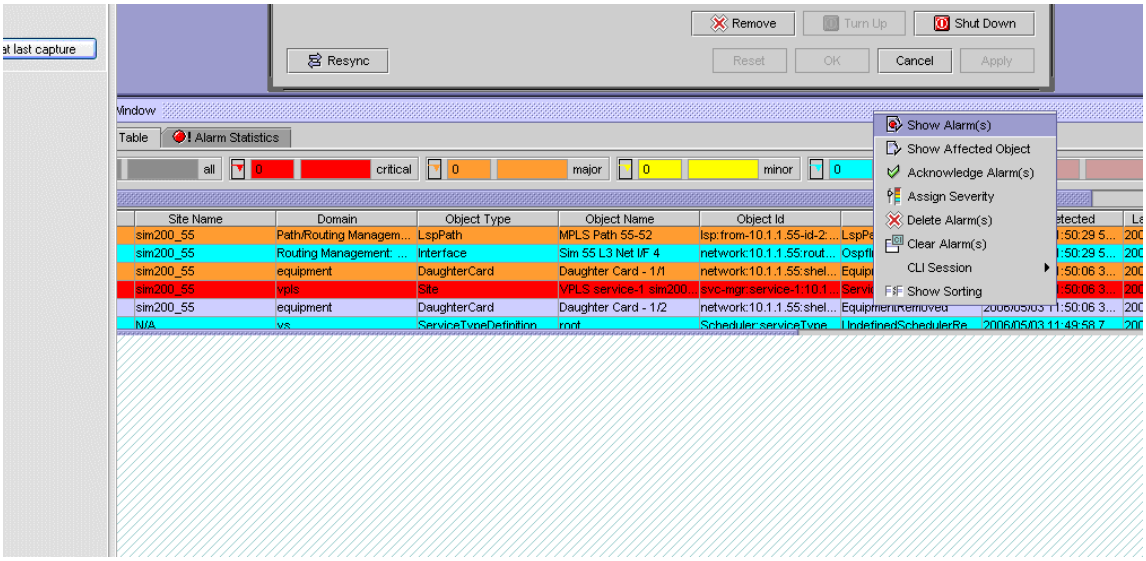
iii Click on the OK button to continue. A check mark appears for the selected alarm under the Ack. column in the dynamic alarm list.

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.

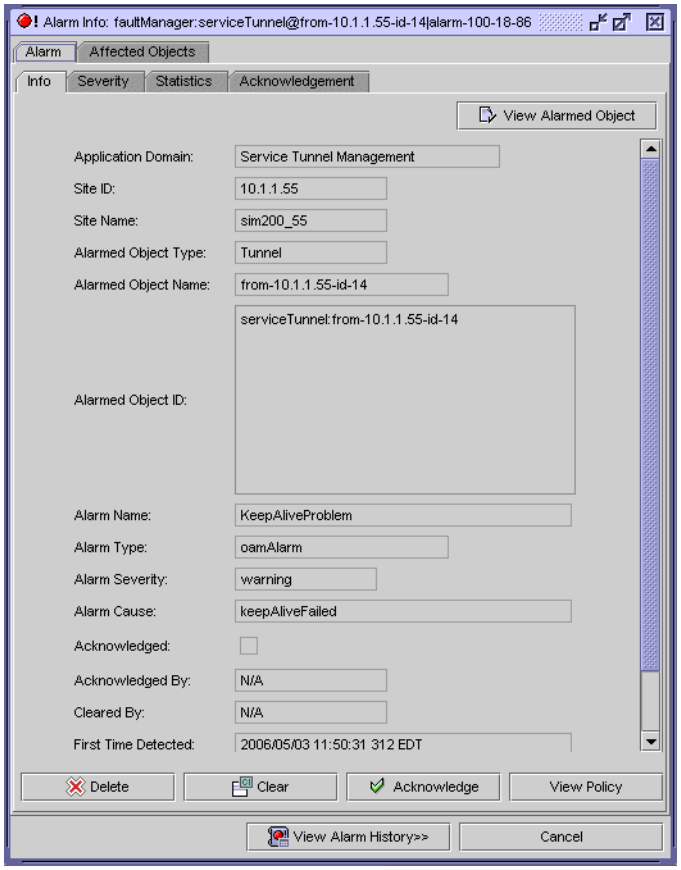
vi Click on the OK button to continue. A check mark appears for each of the selected alarms under the Ack. column in the dynamic alarm list.

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

Alarms are generated by 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.

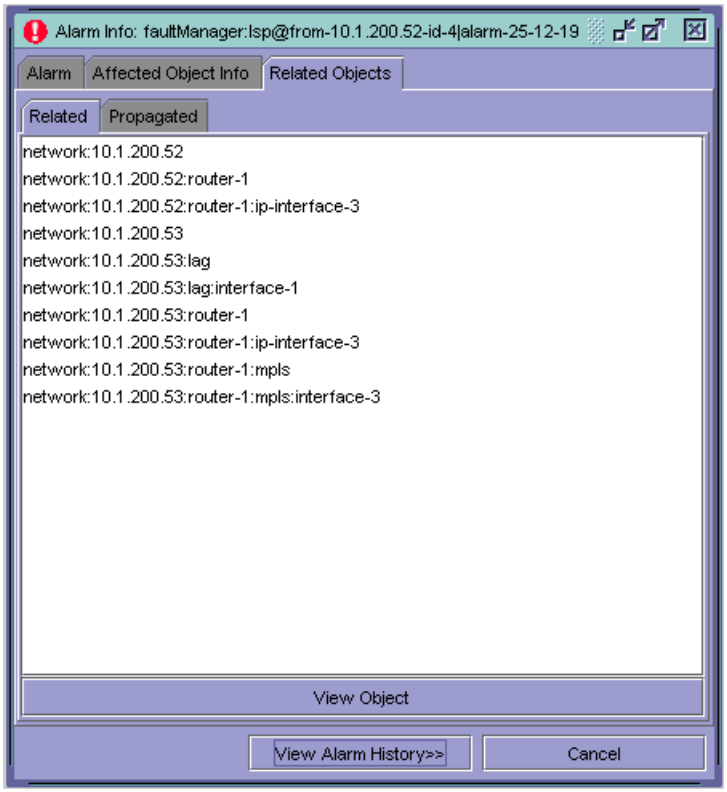
b If the Administrative State is Up and the Operational State is not Up or Down but states a specific problem such as Not Ready or MTU Mismatch, this is the root cause of the alarm. Correct the specified problem and all correlated alarms should clear. See section 3.4 for a sample configuration problem.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

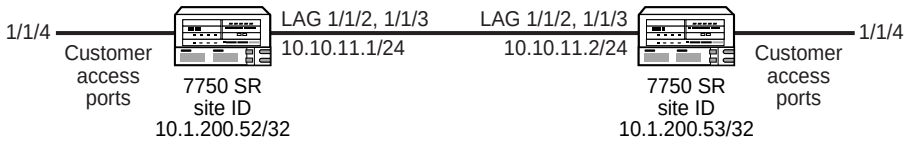
If required, check the Administrative State of the supporting port objects. A port with Administrative State Down does not generate alarms on the port, card, shelf, LAG, protocols, or sessions, but generates network path and service alarms. If the Administrative State is Down, change it to Up.

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



BGP, OSPF, and MPLS are on each network interface.

17558

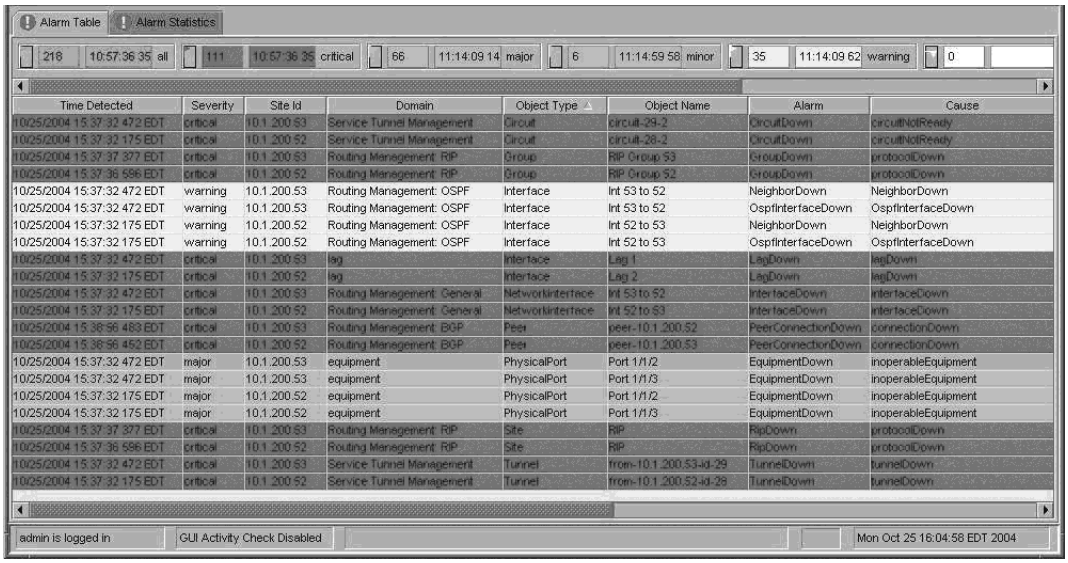
The dynamic alarm list is used to troubleshoot the following types of problems that are created.

- 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 VPLS equipment problem

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

Figure 3-6 VPLS alarm list_1



The following procedure describes how to troubleshoot the problem.

Procedure 3-7 To troubleshoot a VPLS equipment problem

1 Review the alarms in the order that they are generated. When the First Time Detected column or Last Time Generated column shows that the alarms listed are generated 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.

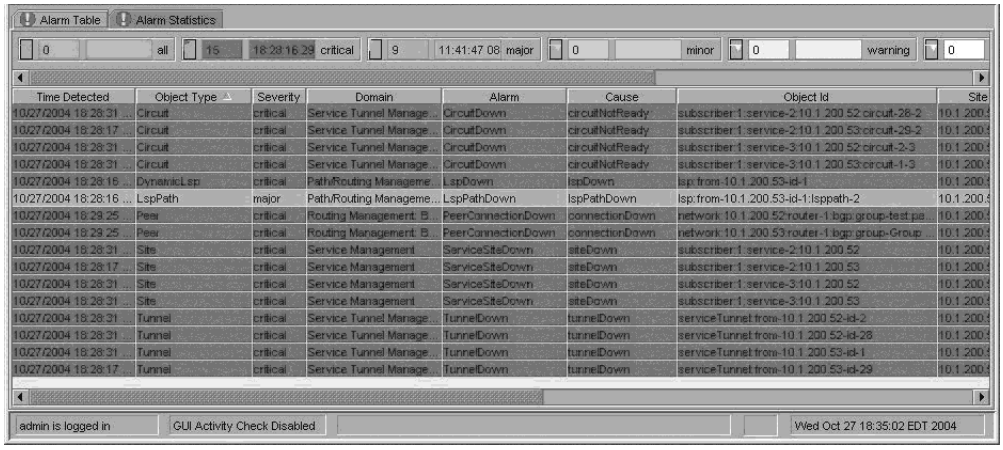
1 Check the physical connection to the port. The physical inspection shows that the two port connections supporting LAG 2 at Site 10.1.200.52. are not properly seated.

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 VPLS 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 generated 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 generated 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 generated 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 3-25 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.

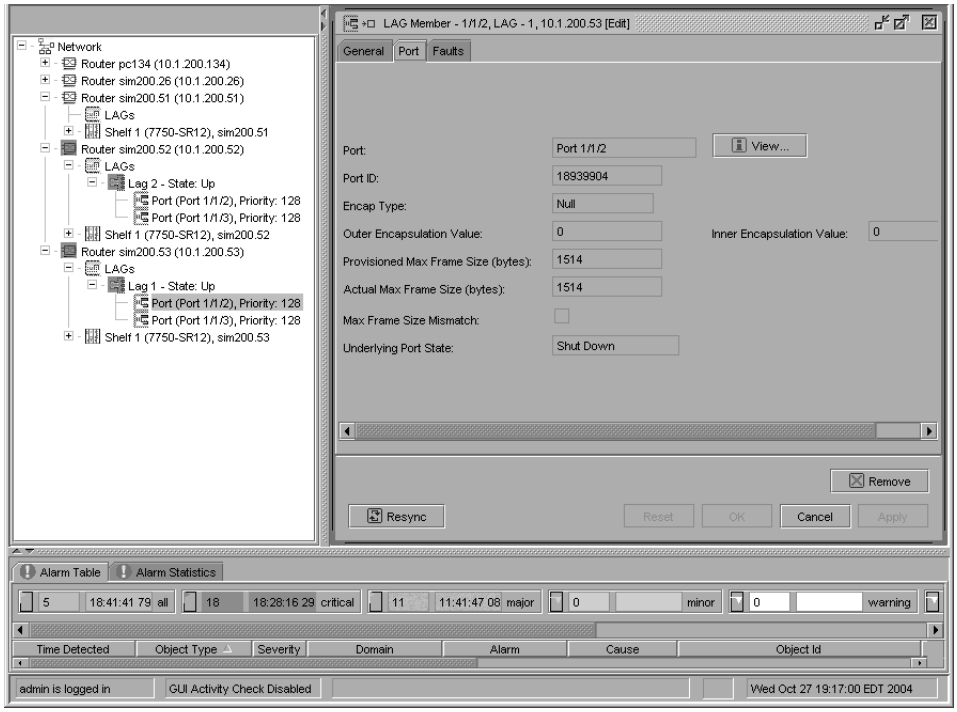
14 Open the equipment view of the navigation tree. It indicates that there are alarms related to both existing LAGs (Site Id 10.1.200.52 and Site Id 10.1.200.53). However, there is no LAG alarm in the dynamic alarm list and the LAG State is Up.

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.

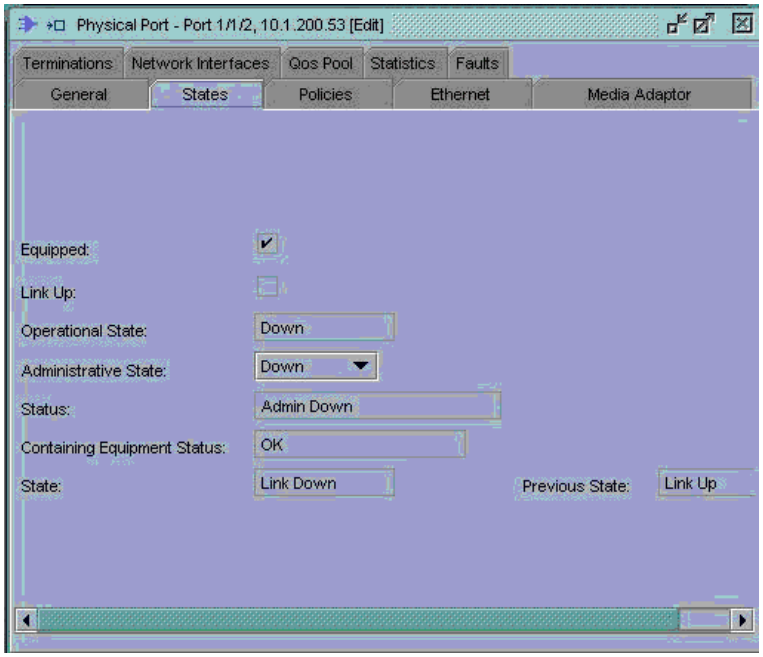
Figure 3-8 LAG member underlying port state in Properties form



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.

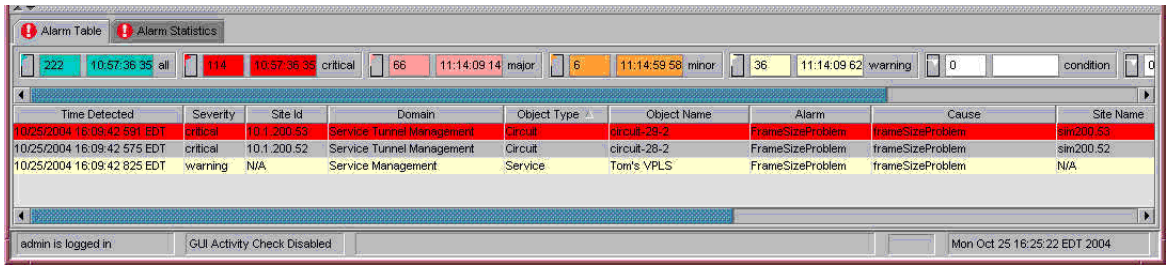
4 Click on the Resync button. An Object Deleted notification appears and the alarm clears automatically.

5 Repeat Steps 3 and 4 for the remaining alarm.

Troubleshooting a VPLS configuration problem

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

Figure 3-10 VPLS alarm list_3



The following procedure describes how to troubleshoot the problem.

Procedure 3-11 To troubleshoot a VPLS configuration problem

1 Review the alarms in the order that they were generated. The First Time Detected column shows that three alarms were generated 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 3-47 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 parameters 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.

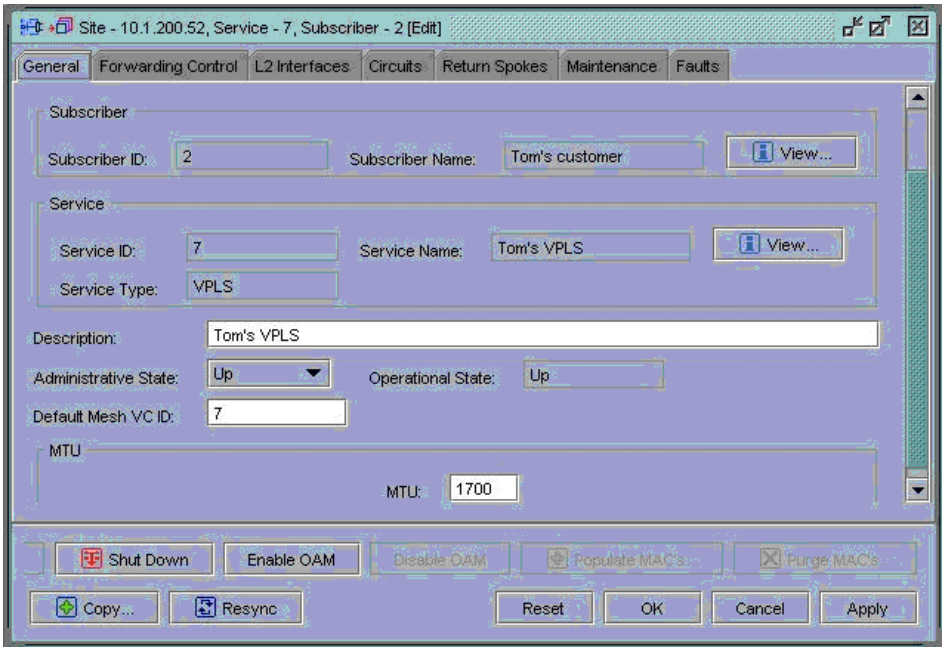
4 Click on the Properties button. The Service form opens.

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

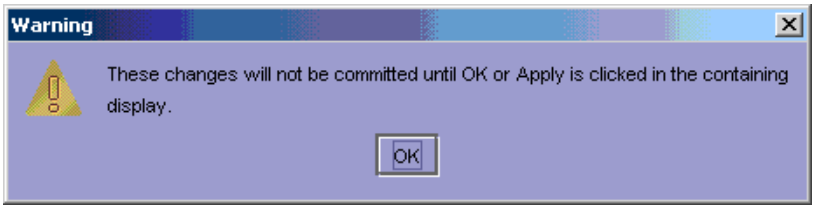


The MTU parameter indicates that the SDP binding maximum frame size is greater than the actual tunnel frame size of 1492 octets that supports the SDP binding.

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, Figure 3-12, 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

Alarms are grouped by domain. Tables 3-2 to 3-57 describe the network-object alarms that the 5620 SAM raises and are listed in alphabetical order by domain. The alarms within a table are in alphabetical order.

A number in parentheses indicates the numeric identifier of an alarm type. For example, “Type: configurationAlarm (11)” indicates that the alarm is a configuration alarm, and the numeric identifier for this type of alarm is 11.

Table 3-2 Domain: antispoof

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: SapStaticHostDynamicMacConflict Alarm ID: 313 Type: configurationAlarm (11) Probable causes: LearnedDynamicMacAlreadyLearned (243)	Severity: minor Object Type (class): AntiSpoofingStaticHosts Domain: antispoof Self-clearing alarm raised: No	—

Table 3-3 Domain: aps

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: AsymmetricalConfig Alarm ID: 295 Type: configurationAlarm (11) Probable causes: asymmetricalConfig (226)	Severity: major Object Type (class): MultiChassisApsGroupContainer Domain: aps Self-clearing alarm raised: Yes	—
Alarm name: IncompleteConfig Alarm ID: 294 Type: configurationAlarm (11) Probable causes: incompleteConfig (225)	Severity: major Object Type (class): MultiChassisApsGroupContainer Domain: aps Self-clearing alarm raised: Yes	—

Table 3-4 Domain: bgp

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: BgpDown Alarm ID: 6 Type: ProtocolAlarm (1) Probable causes: protocolDown (1)	Severity: critical Object Type (class): Site Domain: bgp Self-clearing alarm raised: Yes	—
Alarm name: PeerConnectionDown Alarm ID: 2 Type: ProtocolAlarm (1) Probable causes: connectionDown (2)	Severity: critical Object Type (class): Peer Domain: bgp Self-clearing alarm raised: Yes	Alarm is raised when the BGP peer has a connection state other than established, and the administrative state of the BGP peer is up.
Alarm name: PeerDown Alarm ID: 1 Type: ProtocolAlarm (1) Probable causes: protocolDown (1)	Severity: critical Object Type (class): Peer Domain: bgp Self-clearing alarm raised: Yes	Alarm is raised when the BGP peer has an operational state other than up, and the administrative state is up.
Alarm name: PeerGroupDown Alarm ID: 5 Type: ProtocolAlarm (1) Probable causes: protocolDown (1)	Severity: critical Object Type (class): PeerGroup Domain: bgp Self-clearing alarm raised: Yes	—
Alarm name: PrefixLimitExceeded Alarm ID: 4 Type: ProtocolAlarm (1) Probable causes: prefixLimitExceeded (4)	Severity: critical Object Type (class): Peer Domain: bgp Self-clearing alarm raised: No	The prefix-limit is the maximum number of routes BGP can learn from a peer. The alarm is raised when the maximum number of peer routes has been learned.
Alarm name: PrefixLimitNearing Alarm ID: 3 Type: ProtocolAlarm (1) Probable causes: prefixLimitNearing (3)	Severity: major Object Type (class): Peer Domain: bgp Self-clearing alarm raised: No	The prefix limit is the maximum number of routes BGP can learn from a peer. The alarm is raised when 90% of the maximum allowed peer routes are learned.

Table 3-5 Domain: bundle

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: BundleDown Alarm ID: 152 Type: equipmentAlarm (3) Probable causes: bundleDown (128)	Severity: critical Object Type (class): Interface Domain: bundle Self-clearing alarm raised: Yes	Represents the grouping of T1 and E1 channels into a channel group. The channel group is used as a SAP. The alarm occurs if the interface Administrative State is Up and the Operational State is Down.

Table 3-6 Domain: ccag

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: CcagDown Alarm ID: 210 Type: equipmentAlarm (3) Probable causes: CcagDown (163)	Severity: major Object Type (class): CrossConnectAggregationGroup Domain: ccag Self-clearing alarm raised: Yes	—

Table 3-7 Domain: circem

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: BatmPWVcCurrentFarEndFC Alarm ID: 324 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): Interface Domain: circem Self-clearing alarm raised: No	—
Alarm name: BatmPWVcCurrentJtrBfrOverruns Alarm ID: 318 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): Interface Domain: circem Self-clearing alarm raised: No	—
Alarm name: BatmPWVcCurrentJtrBfrUnderruns Alarm ID: 316 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): Interface Domain: circem Self-clearing alarm raised: No	—
Alarm name: BatmPWVcCurrentMalformedPkt Alarm ID: 320 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): Interface Domain: circem Self-clearing alarm raised: No	—
Alarm name: BatmPWVcCurrentNearEndFC Alarm ID: 322 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): Interface Domain: circem Self-clearing alarm raised: No	—
Alarm name: BatmPWVcCurrentPktsOoseq Alarm ID: 314 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): Interface Domain: circem Self-clearing alarm raised: No	—
Alarm name: BatmPWVcFarEndFC Alarm ID: 325 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): Interface Domain: circem Self-clearing alarm raised: No	—

(1 of 2)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: BatmPWVcJtrBfrOverruns Alarm ID: 319 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): Interface Domain: circem Self-clearing alarm raised: No	—
Alarm name: BatmPWVcJtrBfrUnderruns Alarm ID: 317 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): Interface Domain: circem Self-clearing alarm raised: No	—
Alarm name: BatmPWVcMalformedPkt Alarm ID: 321 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): Interface Domain: circem Self-clearing alarm raised: No	—
Alarm name: BatmPWVcNearEndFC Alarm ID: 323 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): Interface Domain: circem Self-clearing alarm raised: No	—
Alarm name: BatmPWVcPktsOoseq Alarm ID: 315 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): Interface Domain: circem Self-clearing alarm raised: No	—

(2 of 2)

Table 3-8 Domain: db

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: AllArchiveLogsDeleted Alarm ID: 199 Type: databaseAlarm (29) Probable causes: archivedLogsIssue (154)	Severity: warning Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: No	—
Alarm name: ArchiveLogDiskSpaceBelowThreshold Alarm ID: 197 Type: databaseAlarm (29) Probable causes: diskSpaceIssue (153)	Severity: major Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: No	One or more filesystem thresholds for the 5620 SAM database have been reached, as specified in the nms-server.xml file.
Alarm name: BackupDiskSpaceBelowThreshold Alarm ID: 195 Type: databaseAlarm (29) Probable causes: diskSpaceIssue (153)	Severity: major Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: No	

(1 of 4)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: DatabaseArchivedLogNotApplied Alarm ID: 205 Type: configurationAlarm (11) Probable causes: databaseArchivedLogNotApplied (159)	Severity: warning Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: No	—
Alarm name: DatabaseBackupFailed Alarm ID: 136 Type: configurationAlarm (11) Probable causes: databaseBackupFailure (109)	Severity: major Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: No	The backup file could not be created because of, for example, lack of disk space or invalid write permissions.
Alarm name: DatabaseRedundancyFailure Alarm ID: 246 Type: configurationAlarm (11) Probable causes: DatabaseRedundancyFailure (184)	Severity: major Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: No	The alarm is raised when a problem is detected with the standby (secondary) database. Possible problem states include: • down • out of synchronization • old primary due to a failover • not in managed recovery mode When the standby database server is online and the former active comes online as the standby, you can manually clear the alarm.
Alarm name: DatabaseRedundancyOutOfSync Alarm ID: 302 Type: configurationAlarm (11) Probable causes: DatabaseRedundancyOutOfSync (233)	Severity: warning Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: No	—
Alarm name: DatabaseRedundancyRealTimeApplyFailure Alarm ID: 296 Type: configurationAlarm (11) Probable causes: DatabaseRedundancyRealTimeApplyFailure (227)	Severity: warning Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: No	This alarm is raised when database redundancy falls out of real-time apply transfer mode, which means that primary database transactions are not immediately replicated to the standby database. The alarm is cleared when the database is again operating in real-time apply mode.
Alarm name: DataFileDiskSpaceBelowThreshold Alarm ID: 196 Type: databaseAlarm (29) Probable causes: diskSpaceIssue (153)	Severity: major Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: Yes	One or more filesystem thresholds for the 5620 SAM database have being reached, as specified in the nms-server.xml file.
Alarm name: DBFailOver Alarm ID: 201 Type: configurationAlarm (11) Probable causes: databasePrimaryDown (155)	Severity: critical Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: No	—

(2 of 4)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: OldArchiveLogsDeleted Alarm ID: 198 Type: databaseAlarm (29) Probable causes: archivedLogsIssue (154)	Severity: warning Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: No	—
Alarm name: OracleHomeDiskSpaceBelowThreshold Alarm ID: 399 Type: databaseAlarm (29) Probable causes: diskSpaceIssue (153)	Severity: major Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: Yes	—
Alarm name: PrimaryDatabaseWasDown Alarm ID: 254 Type: databaseAlarm (29) Probable causes: primaryDatabaseWasDown (193)	Severity: warning Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: No	—
Alarm name: ReinstantiateStandbyDatabase Alarm ID: 252 Type: configurationAlarm (11) Probable causes: reinstantiateStandbyDatabase (191)	Severity: warning Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: No	—
Alarm name: ReinstantiateStandbyDatabaseFailed Alarm ID: 253 Type: configurationAlarm (11) Probable causes: reinstantiateStandbyDatabaseFailed (192)	Severity: critical Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: No	—
Alarm name: RowThresholdConstraintViolated Alarm ID: 286 Type: configurationAlarm (11) Probable causes: partialConstraintEnforcement (218)	Severity: major Object Type (class): SizeConstraintPolicy Domain: db Self-clearing alarm raised: Yes	This alarm is raised when the number of records in a table exceeds the number specified in a size constraint policy. Size constraint policies specify the amount of database capacity that historical records consume. See the 5620 SAM User Guide for more information on size constraint policies.
Alarm name: SwitchOverDatabase Alarm ID: 203 Type: configurationAlarm (11) Probable causes: switchOverDatabase (157)	Severity: warning Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: No	—
Alarm name: SwitchOverDatabaseFailed Alarm ID: 204 Type: configurationAlarm (11) Probable causes: switchOverDatabaseFailed (158)	Severity: critical Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: No	—

(3 of 4)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: TwoPrimaryDatabase Alarm ID: 202 Type: configurationAlarm (11) Probable causes: twoPrimaryDatabase (156)	Severity: critical Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: No	—
Alarm name: UnableDeleteArchivedLogs Alarm ID: 200 Type: databaseAlarm (29) Probable causes: archivedLogsIssue (154)	Severity: warning Object Type (class): DatabaseManager Domain: db Self-clearing alarm raised: No	—

(4 of 4)

Table 3-9 Domain: equipment

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: BatmDsx1CurrentCSSs Alarm ID: 336 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): PhysicalPort Domain: equipment Self-clearing alarm raised: No	—
Alarm name: BatmDsx1CurrentESs Alarm ID: 330 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): PhysicalPort Domain: equipment Self-clearing alarm raised: No	—
Alarm name: BatmDsx1CurrentLESs Alarm ID: 326 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): PhysicalPort Domain: equipment Self-clearing alarm raised: No	—
Alarm name: BatmDsx1CurrentPVCs Alarm ID: 328 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): PhysicalPort Domain: equipment Self-clearing alarm raised: No	—
Alarm name: BatmDsx1CurrentSEFSs Alarm ID: 334 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): PhysicalPort Domain: equipment Self-clearing alarm raised: No	—
Alarm name: BatmDsx1CurrentSESs Alarm ID: 332 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): PhysicalPort Domain: equipment Self-clearing alarm raised: No	—
Alarm name: BatmDsx1CurrentUASs Alarm ID: 338 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): PhysicalPort Domain: equipment Self-clearing alarm raised: No	—

(1 of 5)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: BatmDsx1TotalCSSs Alarm ID: 337 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): PhysicalPort Domain: equipment Self-clearing alarm raised: No	—
Alarm name: BatmDsx1TotalESs Alarm ID: 331 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): PhysicalPort Domain: equipment Self-clearing alarm raised: No	—
Alarm name: BatmDsx1TotalLESs Alarm ID: 327 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): PhysicalPort Domain: equipment Self-clearing alarm raised: No	—
Alarm name: BatmDsx1TotalPVCs Alarm ID: 329 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): PhysicalPort Domain: equipment Self-clearing alarm raised: No	—
Alarm name: BatmDsx1TotalSEFSs Alarm ID: 335 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): PhysicalPort Domain: equipment Self-clearing alarm raised: No	—
Alarm name: BatmDsx1TotalSESs Alarm ID: 333 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): PhysicalPort Domain: equipment Self-clearing alarm raised: No	—
Alarm name: BatmDsx1TotalUASs Alarm ID: 339 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): PhysicalPort Domain: equipment Self-clearing alarm raised: No	—
Alarm name: ConfigNotCompatible Alarm ID: 405 Type: equipmentAlarm (3) Probable causes: DaughterCardConfigNotCompatible (301)	Severity: critical Object Type (class): PhysicalPort Domain: equipment Self-clearing alarm raised: No	—
Alarm name: DataLossAlarm Alarm ID: 148 Type: storageAlarm (25) Probable causes: dataLoss (122)	Severity: major Object Type (class): FlashMemory Domain: equipment Self-clearing alarm raised: Yes	An error has occurred while writing to the compact flash on the router. This indicates a probable data loss. Check the compact flash capacity on the router.
Alarm name: DaughterCardConfigNotCompatible Alarm ID: 404 Type: equipmentAlarm (3) Probable causes: DaughterCardConfigNotCompatible (301)	Severity: critical Object Type (class): DaughterCardSlot Domain: equipment Self-clearing alarm raised: No	—

(2 of 5)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: DiskCapacityProblem Alarm ID: 144 Type: storageAlarm (25) Probable causes: diskCapacityProblem (115)	Severity: variable or indeterminate Object Type (class): FlashMemory Domain: equipment Self-clearing alarm raised: Yes	The compact flash capacity threshold has been reached or exceeded on the NE. These alarms start appearing when capacity reaches 75% or greater. This is a non-configurable threshold value. The alarm condition is detected during resynchronization or upon the receipt of a tnmxEqFlashDiskFull trap. The severity of the alarm is *variable*, depending on the percentage of disk capacity used. When disk capacity equals: • 75% to 89%, severity is minor • 90% to 99%, severity is major • 100%, severity is critical
Alarm name: downgradedCardAlarm Alarm ID: 256 Type: softwareAlarm (19) Probable causes: downgradedCard (195)	Severity: warning Object Type (class): Card Domain: equipment Self-clearing alarm raised: Yes	The downgraded card alarm is raised against IOMs that are not yet reset after the managed device software is upgraded on both CPMs, and the IOM cards are not upgraded or reset, The IOM cards are rebooted automatically after 120 minutes if they are not rebooted manually after a CPM upgrade.
Alarm name: EquipmentDown Alarm ID: 10 Type: equipmentAlarm (3) Probable causes: inoperableEquipment (8)	Severity: major Object Type (class): Equipment Domain: equipment Self-clearing alarm raised: Yes	—
Alarm name: EquipmentFailure Alarm ID: 145 Type: equipmentAlarm (3) Probable causes: fanFailure (116)	Severity: critical Object Type (class): FanTray Domain: equipment Self-clearing alarm raised: Yes	When the object type is ControlProcessor, the failure cause could be that the CPM did not boot. When the object type is a Power Supply Tray, the failure cause could be that a trap is received from the managed device when the: • device is discovered and the power supply tray is out of service • power supply tray of a discovered device goes out of service or the AC power shelf sends a fault message The alarm is cleared when the status changes to OK.
Alarm name: EquipmentInTest Alarm ID: 11 Type: equipmentAlarm (3) Probable causes: equipmentInTest (9)	Severity: warning Object Type (class): Equipment Domain: equipment Self-clearing alarm raised: Yes	This alarm is raised when the equipment enters a diagnostic state.

(3 of 5)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: EquipmentMismatch Alarm ID: 9 Type: equipmentAlarm (3) Probable causes: equipmentTypeMismatch (7)	Severity: major Object Type (class): Equipment Domain: equipment Self-clearing alarm raised: Yes	—
Alarm name: EquipmentRemoved Alarm ID: 8 Type: equipmentAlarm (3) Probable causes: replaceableEquipmentRemoved (6)	Severity: major Object Type (class): Equipment Domain: equipment Self-clearing alarm raised: Yes	—
Alarm name: FirmwareMismatchAlarm Alarm ID: 146 Type: firmwareAlarm (26) Probable causes: bootRomVersionMismatch (119), fpgaVersionMismatch (120)	Severity: critical Object Type (class): Card Domain: equipment Self-clearing alarm raised: Yes	A mismatch occurred between the firmware version and the software image on the router. The alarm lists the expected version.
Alarm name: FirmwareUpgradeAlarm Alarm ID: 212 Type: firmwareAlarm (26) Probable causes: firmwareUpgraded (169)	Severity: SEVERITY_INFO Object Type (class): Card Domain: equipment Self-clearing alarm raised: No	
Alarm name: HardwareRedundancyAlarm Alarm ID: 147 Type: equipmentAlarm (3) Probable causes: primaryCpmFailure (121)	Severity: major Object Type (class): ControlProcessor Domain: equipment Self-clearing alarm raised: Yes	—
Alarm name: LinkDown Alarm ID: 12 Type: communicationsAlarm (4) Probable causes: portLinkProblem (10)	Severity: major Object Type (class): Equipment Domain: equipment Self-clearing alarm raised: Yes	—
Alarm name: OverTemperatureDetected Alarm ID: 388 Type: environmentalAlarm (2) Probable causes: equipmentOverheated (5)	Severity: major Object Type (class): Shelf Domain: equipment Self-clearing alarm raised: Yes	—
Alarm name: SoftwareFailureAlarm Alarm ID: 149 Type: softwareAlarm (19) Probable causes: loadFailed (124)	Severity: critical Object Type (class): ReplaceableUnit Domain: equipment Self-clearing alarm raised: Yes	This alarm is generated when the CPM fails to load the software from the specified location. The alarm lists the location of the software.
Alarm name: SSHServerPreserveKeyFailure Alarm ID: 406 Type: softwareAlarm (19) Probable causes: preserveKeyFailure (302)	Severity: critical Object Type (class): FlashMemory Domain: equipment Self-clearing alarm raised: No	The alarm is generated when the CPM module fails to save the SSH server host key on the persistent drive.

(4 of 5)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: TemperatureThresholdCrossed Alarm ID: 7 Type: environmentalAlarm (2) Probable causes: equipmentOverheated (5)	Severity: major Object Type (class): Environment Domain: equipment Self-clearing alarm raised: Yes	To display the temperature threshold, choose Application->Equipment Manager->Cards tab->Environment.
Alarm name: upgradedCardAlarm Alarm ID: 255 Type: softwareAlarm (19) Probable causes: upgradedCard (194)	Severity: warning Object Type (class): Card Domain: equipment Self-clearing alarm raised: Yes	The upgraded card alarm is raised against the standby CPM when the standby CPM is rebooted and online. The IOM cards are rebooted automatically after 120 minutes if they are not rebooted manually after a CPM upgrade.

(5 of 5)

Table 3-10 Domain: ethernetequipment

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: EthernetPortHighBer Alarm ID: 307 Type: communicationsAlarm (4) Probable causes: HighBer (238)	Severity: major Object Type (class): EthernetPortSpecifics Domain: ethernetequipment Self-clearing alarm raised: Yes	—
Alarm name: EthernetPortLocalFault Alarm ID: 305 Type: communicationsAlarm (4) Probable causes: LocalFault (236)	Severity: major Object Type (class): EthernetPortSpecifics Domain: ethernetequipment Self-clearing alarm raised: Yes	—
Alarm name: EthernetPortNoFrameLock Alarm ID: 306 Type: communicationsAlarm (4) Probable causes: NoFrameLock (237)	Severity: major Object Type (class): EthernetPortSpecifics Domain: ethernetequipment Self-clearing alarm raised: Yes	—
Alarm name: EthernetPortRemoteFault Alarm ID: 304 Type: communicationsAlarm (4) Probable causes: RemoteFault (235)	Severity: major Object Type (class): EthernetPortSpecifics Domain: ethernetequipment Self-clearing alarm raised: Yes	—
Alarm name: EthernetPortSignalFailure Alarm ID: 303 Type: communicationsAlarm (4) Probable causes: SignalFailure (234)	Severity: major Object Type (class): EthernetPortSpecifics Domain: ethernetequipment Self-clearing alarm raised: Yes	—

Table 3-11 Domain: file

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: LogLocFailure Alarm ID: 340 Type: storageAlarm (25) Probable causes: AdminLocFailure (244), BackupLocFailure (245)	Severity: variable or indeterminate Object Type (class): Policy Domain: file Self-clearing alarm raised: No	This alarm is generated when an attempt to create a log or billing file fails.

Table 3-12 Domain: generic

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: DeploymentFailure Alarm ID: 13 Type: deploymentFailure (5) Probable causes: failedToModifyNetworkResource (11)	Severity: minor Object Type (class): GenericObject Domain: generic Self-clearing alarm raised: Yes	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 deployer ID, the requesting user ID, and the deployment type. To troubleshoot a failed deployer, check the deployer configuration using the 5620 SAM client GUI, as described in Procedure 8-4. When an unsuccessful SNMP set operation causes a deployer to fail, the 5620 SAM retrieves information from the NE about the failed deployment and displays it in the Additional Text field of the alarm. 7250 SAS and Telco device deployments fail when more than one configuration terminal mode session is active.
Alarm name: ThresholdCrossingAlarm Alarm ID: 14 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): GenericObject Domain: generic Self-clearing alarm raised: Yes	—
Alarm name: ThresholdCrossingAlarmDbl Alarm ID: 226 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): GenericObject Domain: generic Self-clearing alarm raised: Yes	This alarm is raised when a value crosses a configured rising or falling threshold. The alarm lists current threshold data, the default threshold value, and the threshold name. To view the alarm information from the Faults tab, click on the Alarms on Related Objects tab button.

Table 3-13 Domain: genericne

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: GenericInterfaceLinkDown Alarm ID: 403 Type: equipmentAlarm (3) Probable causes: inoperableEquipment (8)	Severity: major Object Type (class): GenericNeInterface Domain: genericne Self-clearing alarm raised: Yes	—

Table 3-14 Domain: igmp

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: CModeRxQueryMismatch Alarm ID: 160 Type: configurationAlarm (11) Probable causes: InvalidCompatibilityModeofQueryReceieved (130)	Severity: major Object Type (class): Interface Domain: igmp Self-clearing alarm raised: No	This alarm is raised when an IGMP interface receives an IGMP query of a higher version than the version configured on the interface. For example, if the interface is configured as IGMPv1 and it receives an IGMPv2 or IGMPv3 query, the IGMP message is not processed.
Alarm name: IgmpDown Alarm ID: 158 Type: ProtocolAlarm (1) Probable causes: protocolDown (1)	Severity: critical Object Type (class): Site Domain: igmp Self-clearing alarm raised: Yes	—
Alarm name: McacPolicyDropped Alarm ID: 341 Type: communicationsAlarm (4) Probable causes: igmpGroupOnSapDropped (246)	Severity: major Object Type (class): Interface Domain: igmp Self-clearing alarm raised: No	The alarm is generated when an IGMP group is dropped because of the application of a multicast CAC policy.
Alarm name: QueryVerMismatch Alarm ID: 159 Type: configurationAlarm (11) Probable causes: InvalidVersionofQueryMessageReceived (129)	Severity: warning Object Type (class): Interface Domain: igmp Self-clearing alarm raised: No	This alarm is raised when an NE interface configured for IGMPv3 receives a query message for an earlier IGMP version. The NE interface consequently enters an IGMP mode that is compatible with the earlier version. The IGMP version configured on the interface and the version of the received IGMP query are displayed in the additional text of the alarm.

Table 3-15 Domain: ipipe

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: CeAddressIncompatible Alarm ID: 251 Type: configurationAlarm (11) Probable causes: ceAddressIncompatible (190)	Severity: major Object Type (class): Ipipe Domain: ipipe Self-clearing alarm raised: Yes	Alarms are 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 3-16 Domain: isis

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: IsisAdjacencyDown Alarm ID: 153 Type: adjacencyAlarm (31) Probable causes: IsisInterfaceDown (232)	Severity: minor Object Type (class): Interface Domain: isis Self-clearing alarm raised: Yes	—
Alarm name: IsisAreaMismatch Alarm ID: 156 Type: configurationAlarm (11) Probable causes: areaTypeMisconfigured (34)	Severity: warning Object Type (class): Site Domain: isis Self-clearing alarm raised: Yes	—
Alarm name: IsisAuthFailure Alarm ID: 155 Type: authenticationAlarm (14) Probable causes: authFailure (46)	Severity: warning Object Type (class): Site Domain: isis Self-clearing alarm raised: No	—
Alarm name: IsisAuthTypeFailure Alarm ID: 154 Type: authenticationAlarm (14) Probable causes: authFailure (46)	Severity: warning Object Type (class): Site Domain: isis Self-clearing alarm raised: Yes	—
Alarm name: IsisDown Alarm ID: 19 Type: ProtocolAlarm (1) Probable causes: protocolDown (1)	Severity: critical Object Type (class): Site Domain: isis Self-clearing alarm raised: Yes	—
Alarm name: IsisInterfaceDown Alarm ID: 301 Type: ProtocolAlarm (1) Probable causes: protocolDown (1)	Severity: warning Object Type (class): Interface Domain: isis Self-clearing alarm raised: Yes	—

(1 of 2)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: IsisManualAddressDrops Alarm ID: 157 Type: configurationAlarm (11) Probable causes: noError (44)	Severity: warning Object Type (class): Site Domain: isis Self-clearing alarm raised: No	—
Alarm name: IsisRejectedAdjacency Alarm ID: 214 Type: adjacencyAlarm (31) Probable causes: interfaceMismatch (170)	Severity: minor Object Type (class): Interface Domain: isis Self-clearing alarm raised: Yes	—

(2 of 2)

Table 3-17 Domain: l2fwd

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: ForwardingTableSizeLimitReached Alarm ID: 164 Type: resourceAlarm (28) Probable causes: resourceLimitReached (131)	Severity: major Object Type (class): SiteFib Domain: l2fwd Self-clearing alarm raised: Yes	Layer 2 FIB resource problem. Entries in the FIB are derived from the reachability information in the routing information base.
Alarm name: MissingLocalEntry Alarm ID: 291 Type: configurationAlarm (11) Probable causes: Protected_Mac_Address_Not_Global (222)	Severity: minor Object Type (class): ServiceMacProtection Domain: l2fwd Self-clearing alarm raised: Yes	A protected MAC address is distributed to all sites of a VPLS service. The 5620 SAM raises this alarm if a protected MAC address on one of the VPLS sites is removed using CLI.
Alarm name: sapReceivedProtSrcMac Alarm ID: 393 Type: accessInterfaceAlarm (40) Probable causes: ProtectedSourceMacLearned (294)	Severity: minor Object Type (class): AccessInterfaceFib Domain: l2fwd Self-clearing alarm raised: No	—
Alarm name: StpExceptionCondition Alarm ID: 297 Type: AccessInterfaceAlarm (32) Probable causes: StpException (228)	Severity: major Object Type (class): AccessInterfaceStp Domain: l2fwd Self-clearing alarm raised: Yes	This alarm is raised when an STP exception condition is present on a SAP. The node sends a trap to the 5620 SAM when the STP condition has changed. Conditions that can cause this alarm include, one way communication or the detection of a downstream loop.

Table 3-18 Domain: l3fwd

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: DuplicateVrfPolicy Alarm ID: 229 Type: configurationAlarm (11) Probable causes: duplicateVrfPolicyExists (177)	Severity: warning Object Type (class): ServiceSiteImportPolicy Domain: l3fwd Self-clearing alarm raised: Yes	Review the alarm details for additional information about the alarm, including: • the policy number and type • the site Alarm ID and service Alarm ID of the duplicate VRF policy or target
Alarm name: DuplicateVrfTarget Alarm ID: 230 Type: configurationAlarm (11) Probable causes: duplicateVrfTargetExists (178)	Severity: warning Object Type (class): ServiceSite Domain: l3fwd Self-clearing alarm raised: Yes	
Alarm name: ExportPolicyNotFound Alarm ID: 231 Type: configurationAlarm (11) Probable causes: exportPolicyDoesNotExist (179)	Severity: major Object Type (class): ServiceSiteExportPolicy Domain: l3fwd Self-clearing alarm raised: Yes	The alarms list the policy number of the expected policy.
Alarm name: ImportPolicyNotFound Alarm ID: 232 Type: configurationAlarm (11) Probable causes: importPolicyDoesNotExist (180)	Severity: major Object Type (class): ServiceSiteImportPolicy Domain: l3fwd Self-clearing alarm raised: Yes	
Alarm name: MaxNumMcastRoutes Alarm ID: 206 Type: ProtocolAlarm (1) Probable causes: MaxNumMcastRoutesReached (160)	Severity: major Object Type (class): Site Domain: l3fwd Self-clearing alarm raised: Yes	—
Alarm name: McastRoutesMidLevelThresholdReached Alarm ID: 207 Type: ProtocolAlarm (1) Probable causes: MidLevelThresholdReached (161)	Severity: minor Object Type (class): Site Domain: l3fwd Self-clearing alarm raised: No	The alarm lists the number of multicast routes and the threshold value. During VPRN site routing configuration, you can specify the following: • the allowed maximum number of multicast routes for the site • whether the site enforces the allowed maximum number of multicast routes See the VPRN chapter of the *5620 SAM User Guide* for more information about VPRN configuration.
Alarm name: RouteDistinguisherNotConfigured Alarm ID: 142 Type: configurationAlarm (11) Probable causes: routeDistinguisherNotConfigured (113)	Severity: major Object Type (class): ServiceSite Domain: l3fwd Self-clearing alarm raised: Yes	There is a configuration problem on Layer 3 forwarding service site.

Table 3-19 Domain: lag

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: LagDown Alarm ID: 20 Type: equipmentAlarm (3) Probable causes: lagDown (17)	Severity: critical Object Type (class): Interface Domain: lag Self-clearing alarm raised: Yes	All the ports in the LAG are operationally down.
Alarm name: MCLagDown Alarm ID: 394 Type: equipmentAlarm (3) Probable causes: mcLagDown (295)	Severity: critical Object Type (class): MultiChassisLagSpecifics Domain: lag Self-clearing alarm raised: Yes	All the ports in the MC LAG are operationally down.

Table 3-20 Domain: layer2

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: IgmpSnoopingDown Alarm ID: 161 Type: ProtocolAlarm (1) Probable causes: protocolDown (1)	Severity: warning Object Type (class): Bridge Domain: layer2 Self-clearing alarm raised: Yes	—
Alarm name: MvrSiteDown Alarm ID: 162 Type: ProtocolAlarm (1) Probable causes: protocolDown (1)	Severity: warning Object Type (class): MvrSite Domain: layer2 Self-clearing alarm raised: Yes	—
Alarm name: TlsSiteDown Alarm ID: 163 Type: ProtocolAlarm (1) Probable causes: protocolDown (1)	Severity: warning Object Type (class): TlsSite Domain: layer2 Self-clearing alarm raised: Yes	—

Table 3-21 Domain: ldp

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: LdpDown Alarm ID: 22 Type: ProtocolAlarm (1) Probable causes: protocolDown (1)	Severity: critical Object Type (class): Site Domain: ldp Self-clearing alarm raised: Yes	—

(1 of 2)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: LdpInterfaceDown Alarm ID: 21 Type: ProtocolAlarm (1) Probable causes: protocolDown (1)	Severity: critical Object Type (class): Interface Domain: ldp Self-clearing alarm raised: No	—
Alarm name: LdpTargetedPeerDown Alarm ID: 23 Type: ProtocolAlarm (1) Probable causes: protocolDown (1)	Severity: critical Object Type (class): TargetedPeer Domain: ldp Self-clearing alarm raised: Yes	This is an LDP configuration component.

(2 of 2)

Table 3-22 Domain: mediation

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: CorruptImageFile Alarm ID: 171 Type: configurationAlarm (11) Probable causes: invalidOrCorruptImageFile (134)	Severity: critical Object Type (class): SoftwareFolderDescriptor Domain: mediation Self-clearing alarm raised: Yes	The image file indicated in the Software Upgrade Policy in 5620 SAM is corrupt.

Table 3-23 Domain: mirror

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: MirrorDestinationMisconfigured Alarm ID: 209 Type: configurationAlarm (11) Probable causes: mirrorDestinationMisconfigured (162)	Severity: major Object Type (class): Mirror Domain: mirror Self-clearing alarm raised: Yes	More than one destination SAP is configured for a service mirror.
Alarm name: MirrorEncapsulationTypeInconsistent Alarm ID: 217 Type: configurationAlarm (11) Probable causes: mirrorEncapsulationTypeInconsistent (171)	Severity: major Object Type (class): Mirror Domain: mirror Self-clearing alarm raised: Yes	The encapsulation type is inconsistent among the mirroring sites of a service.

Table 3-24 Domain: monpath

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: IpPathMonitorFailedRetryThresholdCrossed Alarm ID: 400 Type: topologyAlarm (34) Probable causes: ipPathCouldNotBeDetermined (299)	Severity: major Object Type (class): MonitoredIpPath Domain: monpath Self-clearing alarm raised: Yes	—
Alarm name: IpPathMonitorRetryAttemptsExhausted Alarm ID: 401 Type: topologyAlarm (34) Probable causes: ipPathCouldNotBeDetermined (299)	Severity: major Object Type (class): MonitoredIpPath Domain: monpath Self-clearing alarm raised: No	—

Table 3-25 Domain: mpls

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: LastHopIncorrectLabelAction Alarm ID: 352 Type: configurationAlarm (11) Probable causes: LabelActionIsNotPopOnLastHop (254)	Severity: warning Object Type (class): StaticLsp Domain: mpls Self-clearing alarm raised: Yes	—
Alarm name: LastHopNotMatchingDestination Alarm ID: 351 Type: configurationAlarm (11) Probable causes: LastHopNotMatchingDestination (253)	Severity: warning Object Type (class): StaticLsp Domain: mpls Self-clearing alarm raised: Yes	—
Alarm name: LspDown Alarm ID: 25 Type: pathAlarm (12) Probable causes: lspDown (19)	Severity: critical Object Type (class): Lsp Domain: mpls Self-clearing alarm raised: Yes	The alarm is raised when the operational state of the LSP is down, but the administrative state is up. Verify the status of the underlying ports as a probable cause. For dynamic LSP signaling, ensure that one of the two supported signaling protocols, either LDP or RSVP, is enabled on the interfaces that support the dynamic creation of LSPs. For static LSPs, if there is no ARP entry for the next-hop IP address of the LSP, the LSP is set to operationally down. Ensure that at least one MPLS interface is configured on the device. Ensure that MPLS is enabled on all devices that are part of an LSP.

(1 of 2)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: LspPathBypassTunnelActive Alarm ID: 264 Type: pathAlarm (12) Probable causes: LspPathReroutedToBypassTunnel (197)	Severity: warning Object Type (class): LspPath Domain: mpls Self-clearing alarm raised: Yes	When an LSP primary path is rerouted to the bypass tunnel, the alarm is raised. When the primary path is returned to the original tunnel and the actual hop returns to the primary path, the alarm is cleared.
Alarm name: LspPathDown Alarm ID: 26 Type: pathAlarm (12) Probable causes: lspPathDown (20)	Severity: major Object Type (class): LspPath Domain: mpls Self-clearing alarm raised: Yes	—
Alarm name: MissingHopConfiguration Alarm ID: 350 Type: configurationAlarm (11) Probable causes: MissingHopConfiguration (252)	Severity: warning Object Type (class): StaticLsp Domain: mpls Self-clearing alarm raised: Yes	—
Alarm name: MplsDown Alarm ID: 27 Type: ProtocolAlarm (1) Probable causes: protocolDown (1)	Severity: critical Object Type (class): Site Domain: mpls Self-clearing alarm raised: Yes	—
Alarm name: PathReoptimized Alarm ID: 28 Type: pathAlarm (12) Probable causes: pathReoptimized (21)	Severity: warning Object Type (class): Tunnel Domain: mpls Self-clearing alarm raised: No	This alarm is raised against an MPLS path when an mplsTunnelReoptimized trap is received from the node.
Alarm name: PathRerouted Alarm ID: 29 Type: pathAlarm (12) Probable causes: pathRerouted (22)	Severity: warning Object Type (class): Tunnel Domain: mpls Self-clearing alarm raised: No	This alarm is raised against an MPLS path when an mplsTunnelRerouted trap is received from the node.
Alarm name: TunnelDown Alarm ID: 30 Type: pathAlarm (12) Probable causes: tunnelDown (23)	Severity: warning Object Type (class): Tunnel Domain: mpls Self-clearing alarm raised: Yes	This alarm is raised against an MPLS path when the MPLS path is administratively up but not operationally up.

(2 of 2)

Table 3-26 Domain: msdp

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: MsdpActSrcLimExcd Alarm ID: 380 Type: communicationsAlarm (4) Probable causes: MsdpActiveSourcesLimitExceeded (279)	Severity: warning Object Type (class): Site Domain: msdp Self-clearing alarm raised: No	The alarm is generated when the number of source active messages received by the MSDP site exceeds the configured maximum.
Alarm name: MsdpDown Alarm ID: 353 Type: ProtocolAlarm (1) Probable causes: protocolDown (1)	Severity: critical Object Type (class): Site Domain: msdp Self-clearing alarm raised: Yes	This alarm is generated when an MSDP site is administratively disabled. The alarm clears when the site is administratively enabled.
Alarm name: MsdpGroupSrcActMsgsExcd Alarm ID: 378 Type: communicationsAlarm (4) Probable causes: MsdpGroupActiveSourcesLimitExceeded (277)	Severity: warning Object Type (class): PeerGroup Domain: msdp Self-clearing alarm raised: No	The alarm is generated when the number of source active messages received by the MSDP group exceeds the configured maximum.
Alarm name: MsdpPeerActSrcLimExcd Alarm ID: 379 Type: communicationsAlarm (4) Probable causes: MsdpPeerActiveSourcesLimitExceeded (278)	Severity: warning Object Type (class): Peer Domain: msdp Self-clearing alarm raised: No	The alarm is generated when the number of source active messages received by the MSDP peer exceeds the configured maximum.
Alarm name: MsdpRPFFailure Alarm ID: 354 Type: communicationsAlarm (4) Probable causes: MsdpRPFFailure (275)	Severity: warning Object Type (class): Site Domain: msdp Self-clearing alarm raised: No	This alarm is generated when an MSDP site experiences an RPF failure.
Alarm name: MsdpSourceSrcActMsgsExcd Alarm ID: 381 Type: communicationsAlarm (4) Probable causes: MsdpSourceActiveSourcesLimitExceeded (280)	Severity: warning Object Type (class): Source Domain: msdp Self-clearing alarm raised: No	The alarm is generated when the number of source active messages received by the MSDP source exceeds the configured maximum.

Table 3-27 Domain: netw

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: ActivitySwitch Alarm ID: 182 Type: communicationsAlarm (4) Probable causes: systemFailed (144)	Severity: critical Object Type (class): NmsSystem Domain: netw Self-clearing alarm raised: No	This a redundant 5620SAM switchover alarm.
Alarm name: BootParametersMisconfigured Alarm ID: 35 Type: configurationAlarm (11) Probable causes: persistentIndexFailure (30), configFileBootFailure (31)	Severity: critical Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: Yes	The SNMP Index Boot Status is not configured to be persistent on the router. See the router CLI menu “show system info” for the current setting.
Alarm name: CliCommandFailure Alarm ID: 402 Type: communicationsAlarm (4) Probable causes: cliCommandFailure (300)	Severity: warning Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	The CliCommandFailure alarm is generated when a command sent via CLI failed on the node.
Alarm name: CliConnectionProblem Alarm ID: 299 Type: communicationsAlarm (4) Probable causes: cliConnectionProblem (230)	Severity: warning Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	—
Alarm name: CliLoginFailed Alarm ID: 298 Type: communicationsAlarm (4) Probable causes: cliLoginFailed (229)	Severity: warning Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	—
Alarm name: CpuUtilizationExceeded Alarm ID: 358 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	—
Alarm name: DuplicateRouterIdProblem Alarm ID: 411 Type: configurationAlarm (11) Probable causes: duplicateRouterId (168)	Severity: critical Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	—
Alarm name: EventsThrottled Alarm ID: 356 Type: communicationsAlarm (4) Probable causes: snmpDaemonOverloaded (141)	Severity: major Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	—

(1 of 8)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: FrequentFullResyncsDueToTrapProblems Alarm ID: 265 Type: communicationsAlarm (4) Probable causes: frequentFullResyncsDueToTrapProblems (198)	Severity: major Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: Yes	The managed device has sent a number of SNMP traps to the 5620 SAM, and some of the traps were lost, possibly because of congestion in the Ethernet or IP infrastructure. The NE is therefore resynchronized to ensure consistency between the 5620 SAM database and the node database. To prevent frequent resynchronziations, SNMP traps may be ignored for a set interval, during which the NE is in stand-down mode. The interval is displayed in the alarm details. After the interval passes, a resynchronization is performed. The alarm text message indicates, in seconds, when the next resynchronization will be performed. The alarm is cleared when the managed device is taken out of stand-down mode.
Alarm name: FtpClientFailure Alarm ID: 357 Type: communicationsAlarm (4) Probable causes: ftpClientFailure (257)	Severity: warning Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	The alarm is generated when the NE sends notification that a file transfer operation initiated by the FTP client has failed because of file unavailability, interruption during the file transfer, or a lack of available storage space.
Alarm name: InBandManagementConnectionDown Alarm ID: 139 Type: communicationsAlarm (4) Probable causes: managementConnectionDown (111)	Severity: critical Object Type (class): NodeDiscoveryControl Domain: netw Self-clearing alarm raised: No	—
Alarm name: InterfaceDown Alarm ID: 36 Type: InterfaceAlarm (13) Probable causes: interfaceDown (32)	Severity: critical Object Type (class): StatefullConnectableInterface Domain: netw Self-clearing alarm raised: Yes	—
Alarm name: JMSServerDown Alarm ID: 360 Type: communicationsAlarm (4) Probable causes: systemFailed (144)	Severity: critical Object Type (class): NmsSystem Domain: netw Self-clearing alarm raised: No	—
Alarm name: ManagementInterfaceProtectionSwitch Alarm ID: 34 Type: communicationsAlarm (4) Probable causes: switchToSecondary (28), switchToPrimary (29)	Severity: warning Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	When a network element has dual management interfaces (in-band and out-of-band), this alarm indicates a switch from out-of-band management to in-band management or vice versa.

(2 of 8)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: MemoryConsumption Alarm ID: 216 Type: communicationsAlarm (4) Probable causes: tooManyTrapsBuffered (173)	Severity: major Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: Yes	This alarm is raised when the following conditions are present. • The number of traps from a particular NE that await processing by the 5620 SAM surpasses the NE red threshold for trap memory management specified in the base configuration of the 5620 SAM server. • The global number of traps that await processing by the 5620 SAM surpasses the yellow 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 one of the following conditions is met. • The number of traps from the NE that await processing falls below the NE red threshold. • The global number of traps that await processing falls below the system yellow threshold. The NE is resynchronized only if required.
Alarm name: MisconfiguredNode Alarm ID: 382 Type: configurationAlarm (11) Probable causes: persistOff (281), noSystemAddress (282)	Severity: major Object Type (class): Topology Domain: netw Self-clearing alarm raised: No	—
Alarm name: MissedStatsCollection Alarm ID: 355 Type: communicationsAlarm (4) Probable causes: noAuxiliaryServersAvailable (256)	Severity: critical Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	—
Alarm name: ModuleOutOfMemory Alarm ID: 180 Type: equipmentAlarm (3) Probable causes: outOfMemory (142)	Severity: critical Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	Described
Alarm name: NodeColdStart Alarm ID: 172 Type: equipmentAlarm (3) Probable causes: nodeColdStart (135)	Severity: warning Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	—

(3 of 8)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: NodeRebooted Alarm ID: 32 Type: equipmentAlarm (3) Probable causes: nodeReboot (25)	Severity: warning Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	—
Alarm name: NodeUpgraded Alarm ID: 178 Type: configurationAlarm (11) Probable causes: upgradedNodeVersion (140)	Severity: SEVERITY_INFO Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	—
Alarm name: NodeVersionMismatch Alarm ID: 177 Type: configurationAlarm (11) Probable causes: DowngradedNodeVersion (139)	Severity: critical Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	After an NE is downgraded, you must unmanage and remanage it to attain full NE functionality and to ensure that the 5620 SAM database contains current information about the NE.
Alarm name: OutOfBandManagementConnectionDown Alarm ID: 138 Type: communicationsAlarm (4) Probable causes: managementConnectionDown (111)	Severity: critical Object Type (class): NodeDiscoveryControl Domain: netw Self-clearing alarm raised: No	—
Alarm name: PersistentIndexParametersMisconfigured Alarm ID: 173 Type: configurationAlarm (11) Probable causes: persistentIndexConfigurationMismatch (136)	Severity: major Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: Yes	The 5620 SAM raises this alarm if persistence is configured to Off in the BOF.
Alarm name: PhysicalLinkPortsMisconfigured Alarm ID: 239 Type: configurationAlarm (11) Probable causes: physicalLinkPortsMisconfigured (181)	Severity: minor Object Type (class): PhysicalLink Domain: netw Self-clearing alarm raised: Yes	The alarm can be raised when there is a mismatch in MTU size between link endpoints and ports. When the MTU is configured to match, the alarm is cleared.
Alarm name: PollDeadlineMissed Alarm ID: 240 Type: configurationAlarm (11) Probable causes: tooManyItemsToPoll (183)	Severity: warning Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	—
Alarm name: PollerProblem Alarm ID: 31 Type: communicationsAlarm (4) Probable causes: resyncFailed (24)	Severity: warning Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: Yes	Unable to poll a network object. Possible causes include: intermittent or no IP connectivity to the network object, incorrect SNMP security parameters, or SNMP is disabled on the router. Non-5620 SAM related polling problems may include physical cabling from the NMS domain to the managed devices, and NIC card issues

(4 of 8)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: RamFreeSpaceExceeded Alarm ID: 359 Type: thresholdCrossed (6) Probable causes: thresholdCrossed (12)	Severity: warning Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	—
Alarm name: RedAlarmThresholdReached Alarm ID: 241 Type: communicationsAlarm (4) Probable causes: tooManyAlarms (182)	Severity: critical Object Type (class): NmsSystem Domain: netw Self-clearing alarm raised: No	The number of outstanding alarms has reached the critical threshold, and alarms are being discarded to keep below system limits.
Alarm name: RedundancySwitchover Alarm ID: 181 Type: equipmentAlarm (3) Probable causes: redundancySwitchover (143)	Severity: warning Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	—
Alarm name: SnmpAuthenticationFailure Alarm ID: 176 Type: authenticationAlarm (14) Probable causes: authFailure (46)	Severity: warning Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	—
Alarm name: SnmpDaemonProblem Alarm ID: 175 Type: communicationsAlarm (4) Probable causes: snmpDaemonError (138)	Severity: critical Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	—
Alarm name: SnmpDown Alarm ID: 410 Type: communicationsAlarm (4) Probable causes: snmpDown (306)	Severity: critical Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	—
Alarm name: SnmpIndexUpdateFailed Alarm ID: 395 Type: SnmpIndexUpdateFailedAlarm (41) Probable causes: SnmpIndexUpdateFailure (296)	Severity: critical Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: Yes	—

(5 of 8)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: SnmpReachabilityProblem Alarm ID: 243 Type: communicationsAlarm (4) Probable causes: SnmpReachabilityTestFailed (176)	Severity: major Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: Yes	The alarm is raised if an SNMP poll of the SysUpTimeAlarm OID fails. The likely cause of the failure is that the SNMP agent on the managed device is not reachable. By default, the 5620 SAM polls the managed devices every 2 min. If the poll fails, the alarm is raised. The alarm is cleared when the SNMP agent is again detected as reachable. The icon that represents the managed device turns from red to green on the 5620 SAM client GUI map. Possible causes of the failed poll include: • congestion on the network management LAN • the devices are too busy to respond to the poll request
Alarm name: SnmpTrapDropped Alarm ID: 179 Type: communicationsAlarm (4) Probable causes: snmpDaemonOverloaded (141)	Severity: warning Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	This alarm is raised when a tmnxTrapDropped notification is received from the NE to indicate that the NE has dropped a trap. This results in a resynchronization of the table associated with the dropped trap.
Alarm name: StandbyCPMManagementConnectionDown Alarm ID: 140 Type: communicationsAlarm (4) Probable causes: managementConnectionDown (111)	Severity: critical Object Type (class): NodeDiscoveryControl Domain: netw Self-clearing alarm raised: No	The 5620 SAM can be configured to regularly ping all network devices at 2-min intervals. When a network device cannot be reached using the ping, an alarm is raised.
Alarm name: StandbyServerStatus Alarm ID: 208 Type: communicationsAlarm (4) Probable causes: systemFailed (144)	Severity: critical Object Type (class): NmsSystem Domain: netw Self-clearing alarm raised: No	—
Alarm name: SystemMemoryConsumption Alarm ID: 225 Type: communicationsAlarm (4) Probable causes: tooManyTrapsBuffered (173)	Severity: critical Object Type (class): NmsSystem Domain: netw Self-clearing alarm raised: No	This alarm is raised when the global number of 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 is cleared when the number of traps that await processing falls below the system red threshold. The NEs are resynchronized only if required.

(6 of 8)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: SystemNameChange Alarm ID: 228 Type: equipmentAlarm (3) Probable causes: systemNameChange (174)	Severity: major Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: Yes	Review the alarm record for additional information, including the old system name and the new system name.
Alarm name: TraceError Alarm ID: 289 Type: equipmentAlarm (3) Probable causes: traceError (221)	Severity: critical Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	The alarm is raised when problems are raised on the managed devices. For example, when IOM unusual error log trace messages are generated on the managed device, an SNMP trap is sent to the 5620 SAM. The 5620 SAM then raises this alarm. The alarm indicates the title of the logged event and details from the message. Alcatel-Lucent recommends that when 5620 SAM operators receive this alarm, they should: • open a Telnet or CLI session to the managed device • review the error log trace history files • contact node technical support staff with details of the event • clear the alarm on 5620 SAM
Alarm name: TrapDestinationMisconfigured Alarm ID: 33 Type: configurationAlarm (11) Probable causes: trapDestinationMisconfigured (26), duplicateTrapLogId (27)	Severity: major Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: Yes	The SNMP trap destination configured on the router is not pointing to 5620 SAM.
Alarm name: TrapMalformed Alarm ID: 135 Type: communicationsAlarm (4) Probable causes: trapSchemaMismatch (108)	Severity: major Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: No	—
Alarm name: TrapRateThresholdExceeded Alarm ID: 412 Type: communicationsAlarm (4) Probable causes: trapRateGreaterThanConfigured (307)	Severity: critical Object Type (class): NmsSystem Domain: netw Self-clearing alarm raised: No	—
Alarm name: UnmanageFailed Alarm ID: 300 Type: discoveryControlAlarm (33) Probable causes: unableToDeleteNode (231)	Severity: warning Object Type (class): NodeDiscoveryControl Domain: netw Self-clearing alarm raised: Yes	This alarm is raised when an attempt to unmanage an NE fails.

(7 of 8)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: UnsupportedNode Alarm ID: 288 Type: configurationAlarm (11) Probable causes: unsupportedNode (219)	Severity: warning Object Type (class): Topology Domain: netw Self-clearing alarm raised: No	The alarm is raised during 5620 SAM network discovery if the 5620 SAM detects a network element running an unsupported node software version. The alarm is raised for each discovery rule element, based on the combination of discovery rule ID and the IP address of the device running the unsupported software version.
Alarm name: UpgradedBuildVersionMismatch Alarm ID: 174 Type: configurationAlarm (11) Probable causes: upgradedImageNotBooted (137)	Severity: warning Object Type (class): NetworkElement Domain: netw Self-clearing alarm raised: Yes	—
Alarm name: YellowAlarmThresholdReached Alarm ID: 245 Type: communicationsAlarm (4) Probable causes: tooManyAlarms (182)	Severity: critical Object Type (class): NmsSystem Domain: netw Self-clearing alarm raised: No	The number of outstanding alarms has reached the yellow threshold, and non-critical alarms are being discarded to keep below system limits.

(8 of 8)

Table 3-28 Domain: ospf

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: AreaTypeMismatch Alarm ID: 38 Type: configurationAlarm (11) Probable causes: areaTypeMisconfigured (34)	Severity: warning Object Type (class): Area Domain: ospf Self-clearing alarm raised: Yes	An OSPF area on one router is configured as NSSA and the same OSPF area on another router is configured as a Stub area (no summary).
Alarm name: InterfaceDbDescriptAuthFailure Alarm ID: 46 Type: authenticationAlarm (14) Probable causes: authTypeMismatch (45), authFailure (46)	Severity: warning Object Type (class): Interface Domain: ospf Self-clearing alarm raised: No	—
Alarm name: InterfaceDbDescriptConfig Alarm ID: 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)	Severity: warning Object Type (class): Interface Domain: ospf Self-clearing alarm raised: No	—

(1 of 6)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: InterfaceHelloAuthFailure Alarm ID: 45 Type: authenticationAlarm (14) Probable causes: authTypeMismatch (45), authFailure (46)	Severity: warning Object Type (class): Interface Domain: ospf Self-clearing alarm raised: No	A router uses the OSPF Hello protocol to discover neighbors. Both the hello authentication key and the hello authentication type on a segment must match. When the hello authentication key is configured, it applies to all levels that are configured for the interface. The hello authentication type enables hello authentication at the interface or level context. Ensure that the authentication type parameter values for the routing interfaces are consistent. The alarms may be generated when the managed devices are negotiating with OSPF neighbors after a link failure or an OSPF configuration change. In this case, manually clear the alarm when the OSPF neighbor status is Full.
Alarm name: InterfaceHelloConfig Alarm ID: 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)	Severity: warning Object Type (class): Interface Domain: ospf Self-clearing alarm raised: No	
Alarm name: InterfaceLsAckAuthFailure Alarm ID: 49 Type: authenticationAlarm (14) Probable causes: authTypeMismatch (45), authFailure (46)	Severity: warning Object Type (class): Interface Domain: ospf Self-clearing alarm raised: No	—
Alarm name: InterfaceLsAckConfig Alarm ID: 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)	Severity: warning Object Type (class): Interface Domain: ospf Self-clearing alarm raised: No	—
Alarm name: InterfaceLsReqAuthFailure Alarm ID: 47 Type: authenticationAlarm (14) Probable causes: authTypeMismatch (45), authFailure (46)	Severity: warning Object Type (class): Interface Domain: ospf Self-clearing alarm raised: No	—
Alarm name: InterfaceLsReqConfig Alarm ID: 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)	Severity: warning Object Type (class): Interface Domain: ospf Self-clearing alarm raised: No	—

(2 of 6)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: InterfaceLsUpdateAuthFailure Alarm ID: 48 Type: authenticationAlarm (14) Probable causes: authTypeMismatch (45), authFailure (46)	Severity: warning Object Type (class): Interface Domain: ospf Self-clearing alarm raised: No	—
Alarm name: InterfaceLsUpdateConfig Alarm ID: 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)	Severity: warning Object Type (class): Interface Domain: ospf Self-clearing alarm raised: No	—
Alarm name: InterfaceNullPacketAuthFailure Alarm ID: 50 Type: authenticationAlarm (14) Probable causes: authTypeMismatch (45), authFailure (46)	Severity: warning Object Type (class): Interface Domain: ospf Self-clearing alarm raised: No	—
Alarm name: InterfaceNullPacketConfig Alarm ID: 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)	Severity: warning Object Type (class): Interface Domain: ospf Self-clearing alarm raised: No	—
Alarm name: InterfaceRxBadPacket Alarm ID: 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 Self-clearing alarm raised: No	—
Alarm name: InterfaceTxRetransmit Alarm ID: 52 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 Self-clearing alarm raised: No	The retransmit-interval for OSPF area interface determines how long (in seconds) OSPF waits before retransmitting an unacknowledged LSA to an OSPF neighbor. This alarm is not generated on a 7450 ESS or 7750 SR, Release 4.0 or newer.

(3 of 6)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: LsdbOverflow Alarm ID: 53 Type: equipmentAlarm (3) Probable causes: resourceFull (53)	Severity: major Object Type (class): Site Domain: ospf Self-clearing alarm raised: No	This alarm is raised when the number of received external LSAs exceeds the configured number of allowed external LSAs (by default there is no limit). The configured LSDB limit and the LSDB overflow state (0 = ok, 1 = approaching limit, 2 = limit exceeded) are displayed in the additional text of the alarm.
Alarm name: NeighborDown Alarm ID: 121 Type: NeighborDown (20) Probable causes: NeighborDown (103)	Severity: warning Object Type (class): Interface Domain: ospf Self-clearing alarm raised: Yes	—
Alarm name: OspfInterfaceDown Alarm ID: 141 Type: OspfInterfaceDown (24) Probable causes: OspfInterfaceDown (112)	Severity: warning Object Type (class): Interface Domain: ospf Self-clearing alarm raised: Yes	—
Alarm name: TxRetransmit Alarm ID: 266 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 Self-clearing alarm raised: No	The alarm lists the router ID of the OSPF neighbor device. This alarm is not generated on a 7450 ESS or 7750 SR, Release 4.0 or newer.
Alarm name: VirtualLinkDbDescriptAuthFailure Alarm ID: 61 Type: authenticationAlarm (14) Probable causes: authTypeMismatch (45), authFailure (46)	Severity: warning Object Type (class): VirtualLink Domain: ospf Self-clearing alarm raised: No	—
Alarm name: VirtualLinkDbDescriptConfig Alarm ID: 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)	Severity: warning Object Type (class): VirtualLink Domain: ospf Self-clearing alarm raised: No	—
Alarm name: VirtualLinkDown Alarm ID: 122 Type: VirtualLinkAlarm (21) Probable causes: VirtualLinkDown (104)	Severity: warning Object Type (class): VirtualLink Domain: ospf Self-clearing alarm raised: Yes	—
Alarm name: VirtualLinkHelloAuthFailure Alarm ID: 60 Type: authenticationAlarm (14) Probable causes: authTypeMismatch (45), authFailure (46)	Severity: warning Object Type (class): VirtualLink Domain: ospf Self-clearing alarm raised: No	—

(4 of 6)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: VirtualLinkHelloConfig Alarm ID: 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)	Severity: warning Object Type (class): VirtualLink Domain: ospf Self-clearing alarm raised: No	—
Alarm name: VirtualLinkLsAckAuthFailure Alarm ID: 64 Type: authenticationAlarm (14) Probable causes: authTypeMismatch (45), authFailure (46)	Severity: warning Object Type (class): VirtualLink Domain: ospf Self-clearing alarm raised: No	—
Alarm name: VirtualLinkLsAckConfig Alarm ID: 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)	Severity: warning Object Type (class): VirtualLink Domain: ospf Self-clearing alarm raised: No	—
Alarm name: VirtualLinkLsReqAuthFailure Alarm ID: 62 Type: authenticationAlarm (14) Probable causes: authTypeMismatch (45), authFailure (46)	Severity: warning Object Type (class): VirtualLink Domain: ospf Self-clearing alarm raised: No	—
Alarm name: VirtualLinkLsReqConfig Alarm ID: 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)	Severity: warning Object Type (class): VirtualLink Domain: ospf Self-clearing alarm raised: No	—
Alarm name: VirtualLinkLsUpdateAuthFailure Alarm ID: 63 Type: authenticationAlarm (14) Probable causes: authTypeMismatch (45), authFailure (46)	Severity: warning Object Type (class): VirtualLink Domain: ospf Self-clearing alarm raised: No	—

(5 of 6)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: VirtualLinkLsUpdateConfig Alarm ID: 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)	Severity: warning Object Type (class): VirtualLink Domain: ospf Self-clearing alarm raised: No	—
Alarm name: VirtualLinkNullPacketAuthFailure Alarm ID: 65 Type: authenticationAlarm (14) Probable causes: authTypeMismatch (45), authFailure (46)	Severity: warning Object Type (class): VirtualLink Domain: ospf Self-clearing alarm raised: No	—
Alarm name: VirtualLinkNullPacketConfig Alarm ID: 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)	Severity: warning Object Type (class): VirtualLink Domain: ospf Self-clearing alarm raised: No	—
Alarm name: VirtualLinkRxBadPacket Alarm ID: 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 Self-clearing alarm raised: No	—
Alarm name: VirtualLinkTxRetransmit Alarm ID: 67 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 Self-clearing alarm raised: No	This alarm is not generated on a 7450 ESS or 7750 SR, Release 4.0 or newer.
Alarm name: VirtualNeighborDown Alarm ID: 123 Type: VirtualNeighborDown (22) Probable causes: VirtualNeighborDown (105)	Severity: warning Object Type (class): VirtualLink Domain: ospf Self-clearing alarm raised: Yes	—

(6 of 6)

Table 3-29 Domain: pim

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: DataMtReused Alarm ID: 361 Type: dataMtReusedAlarm (37) Probable causes: DataMtReused (258)	Severity: warning Object Type (class): DataMtInterface Domain: pim Self-clearing alarm raised: No	—
Alarm name: GroupInSSMRange Alarm ID: 187 Type: configurationAlarm (11) Probable causes: STARGGroupInSSMRange (147)	Severity: warning Object Type (class): Site Domain: pim Self-clearing alarm raised: No	The alarm lists additional information, including the source and group IP address, and the message type.
Alarm name: InvalidJoinPrune Alarm ID: 185 Type: communicationsAlarm (4) Probable causes: InvalidJoinPruneReceived (145)	Severity: warning Object Type (class): Site Domain: pim Self-clearing alarm raised: No	
Alarm name: InvalidRegister Alarm ID: 186 Type: communicationsAlarm (4) Probable causes: InvalidJoinRegisterReceived (146)	Severity: warning Object Type (class): Site Domain: pim Self-clearing alarm raised: No	
Alarm name: invalidRPLoopbackInterfaceConfig Alarm ID: 269 Type: configurationAlarm (11) Probable causes: invalidRPLoopbackIfConfig (201)	Severity: warning Object Type (class): VirtualAnyCastRP Domain: pim Self-clearing alarm raised: Yes	—
Alarm name: mismatchAnyCastRPTypes Alarm ID: 270 Type: configurationAlarm (11) Probable causes: mismatchAnyCastRPTypes (202)	Severity: warning Object Type (class): AnyCastRP Domain: pim Self-clearing alarm raised: No	—
Alarm name: missingStaticRPConfigurations Alarm ID: 268 Type: configurationAlarm (11) Probable causes: missingStaticRPConfigurations (200)	Severity: warning Object Type (class): VirtualAnyCastRP Domain: pim Self-clearing alarm raised: Yes	—
Alarm name: NeighborLoss Alarm ID: 188 Type: communicationsAlarm (4) Probable causes: NeighborConnectionLost (148)	Severity: warning Object Type (class): Interface Domain: pim Self-clearing alarm raised: Yes	—

(1 of 2)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: peerSetConfigurationIssue Alarm ID: 267 Type: configurationAlarm (11) Probable causes: mismatchPeerSets (199)	Severity: major Object Type (class): VirtualAnyCastRP Domain: pim Self-clearing alarm raised: Yes	—
Alarm name: PimDown Alarm ID: 184 Type: ProtocolAlarm (1) Probable causes: protocolDown (1)	Severity: critical Object Type (class): Site Domain: pim Self-clearing alarm raised: Yes	—

(2 of 2)

Table 3-30 Domain: policy

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: DefaultInstanceInconsistency Alarm ID: 211 Type: ConfigurationAlarm (15) Probable causes: multipleDefaultInstancesEncountered (54)	Severity: warning Object Type (class): Manager Domain: policy Self-clearing alarm raised: Yes	An accounting policy can specify a default policy for Network and Service policies. The 5620 SAM raises this alarm if an accounting policy is the default for more then one service type or more then one network type.
Alarm name: TemplateInconsistency Alarm ID: 189 Type: ConfigurationAlarm (15) Probable causes: templatePolicyMismatch (149)	Severity: warning Object Type (class): PolicyDefinition Domain: policy Self-clearing alarm raised: Yes	The 5620 SAM raises this alarm if there is a mismatch of data or properties between a global policy and a local node policy.

Table 3-31 Domain: ppp

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: PppLoopbackDetected Alarm ID: 362 Type: configurationAlarm (11) Probable causes: PppLoopbackDetected (259)	Severity: major Object Type (class): Interface Domain: ppp Self-clearing alarm raised: Yes	—

Table 3-32 Domain: radiusaccounting

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: RadisuAcctPlcyFailure Alarm ID: 363 Type: radiusAccountingPolicyAlarm (38) Probable causes: radiusAccountingRequestFailure (260)	Severity: major Object Type (class): Policy Domain: radiusaccounting Self-clearing alarm raised: No	The alarm is generated when a RADIUS accounting request is not successfully sent to any of the RADIUS servers specified in the RADIUS accounting policy.

Table 3-33 Domain: ressubscr

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: HostConnectivityLostRateExceeded Alarm ID: 276 Type: communicationsAlarm (4) Probable causes: hostDown (208), trapDropped (209)	Severity: major Object Type (class): ShcvSite Domain: ressubscr Self-clearing alarm raised: No	The number of SHCV host connectivity loss events that is defined as the maximum permitted for a SAP has been exceeded. If the specified SHCV action is to remove the host information, the host information is removed and the host is not tested for connectivity again.

Table 3-34 Domain: rip

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: GroupDown Alarm ID: 69 Type: ProtocolAlarm (1) Probable causes: protocolDown (1)	Severity: critical Object Type (class): Group Domain: rip Self-clearing alarm raised: Yes	—
Alarm name: RipAuthenticationFailure Alarm ID: 70 Type: authenticationAlarm (14) Probable causes: authFailure (46)	Severity: warning Object Type (class): Interface Domain: rip Self-clearing alarm raised: No	The alarm indicates the peer address.
Alarm name: RipAuthenticationMismatch Alarm ID: 71 Type: authenticationAlarm (14) Probable causes: authTypeMismatch (45)	Severity: warning Object Type (class): Interface Domain: rip Self-clearing alarm raised: No	The alarm indicates the peer address.
Alarm name: RipDown Alarm ID: 72 Type: ProtocolAlarm (1) Probable causes: protocolDown (1)	Severity: critical Object Type (class): Site Domain: rip Self-clearing alarm raised: Yes	—

Table 3-35 Domain: rmon

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: MissingFallingEvent Alarm ID: 414 Type: configurationAlarm (11) Probable causes: incompleteConfig (225)	Severity: major Object Type (class): Alarm Domain: rmon Self-clearing alarm raised: No	—
Alarm name: MissingRisingEvent Alarm ID: 413 Type: configurationAlarm (11) Probable causes: incompleteConfig (225)	Severity: major Object Type (class): Alarm Domain: rmon Self-clearing alarm raised: No	—

Table 3-36 Domain: rsvp

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: RsvpDown Alarm ID: 74 Type: ProtocolAlarm (1) Probable causes: protocolDown (1)	Severity: critical Object Type (class): Site Domain: rsvp Self-clearing alarm raised: Yes	—
Alarm name: SessionDown Alarm ID: 73 Type: ProtocolAlarm (1) Probable causes: interfaceDown (32)	Severity: critical Object Type (class): Session Domain: rsvp Self-clearing alarm raised: Yes	—

Table 3-37 Domain: rtr

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: SubscrAuthPolicyMisconfigured Alarm ID: 271 Type: ConfigurationAlarm (15) Probable causes: SubscrAuthPolicyNotFound (203)	Severity: warning Object Type (class): DhcpRelayConfiguration Domain: rtr Self-clearing alarm raised: Yes	—

Table 3-38 Domain: rules

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: RuleRegistrationError Alarm ID: 364 Type: ConfigurationAlarm (15) Probable causes: ruleContentsError (261)	Severity: warning Object Type (class): RuleSet Domain: rules Self-clearing alarm raised: Yes	—

Table 3-39 Domain: sas

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: SasThresholdExceededAlarm Alarm ID: 272 Type: oamAlarm (18) Probable causes: networkDegradation (204)	Severity: major Object Type (class): Test Domain: sas Self-clearing alarm raised: Yes	Alarms are raised when a rising or falling threshold is crossed due to rising or falling values, based on jitter, latency, or loss. Alarms are raised against scheduled tests only. You can also view the alarm information from the Faults tab. Click on the Alarms on Related Objects tab button for the appropriate tested object against which the threshold was exceeded. Details of the alarm include: • threshold-crossing type • current data on the threshold • current threshold parameter setting, which was exceeded or dropped below, causing the alarm to be raised
Alarm name: SasTooManyTestsOnNodeAlarm Alarm ID: 287 Type: oamAlarm (18) Probable causes: tooManyTestsDeployedOnNode (220)	Severity: major Object Type (class): NeAgent Domain: sas Self-clearing alarm raised: Yes	The alarm displays additional information: • node ID of the managed device with too many tests • the number of deployed tests of the managed device • the maximum number of deployed tests of the managed device When 60% of a node limit for creating or performing OAM tests is reached, the alarm is raised. For individual OAM tests, an attempt to create or perform an NE schedulable test is rejected on a node when the limit of tests reaches 95% of device capacity.

Table 3-40 Domain: security

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: AuthenticationFailure Alarm ID: 128 Type: communicationsAlarm (4) Probable causes: multipleFailedLoginAttempts (107)	Severity: warning Object Type (class): TSecurityManager Domain: security Self-clearing alarm raised: Yes	At lease five attempts to log in to a 5620 SAM client have failed. The alarm contains the name of the user attempting authentication. When the user account of the user is deleted, the alarm is deleted.
Alarm name: KeyChainAuthFailure Alarm ID: 421 Type: communicationsAlarm (4) Probable causes: keyChainAuthFailure (314)	Severity: major Object Type (class): KeyChain Domain: security Self-clearing alarm raised: No	The alarm is generated when the incoming packet is dropped due to key chain authentication failure. Failure could be due to the following: • A send packet did not authorize the keychain but the receive side had enabled the keychain. • Keychain key ID's did not match. • Keychain key digest mismatch. • A packet was received with an invalid enhanced authentication option length. • For other causes of failure refer to *draft-bonica-tcp-auth-05.txt*

(1 of 6)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: Licensed7250LimitExceeded Alarm ID: 233 Type: licensingAlarm (23) Probable causes: licensedLimitExceeded (106)	Severity: critical Object Type (class): License Domain: security Self-clearing alarm raised: Yes	Choose Help->5620 SAM License Information to display the 5620 SAM licence information.
Alarm name: Licensed7250LimitNearing Alarm ID: 234 Type: licensingAlarm (23) Probable causes: licensedLimitNearing (132)	Severity: warning Object Type (class): License Domain: security Self-clearing alarm raised: Yes	
Alarm name: Licensed7250LimitNearlyExceeded Alarm ID: 235 Type: licensingAlarm (23) Probable causes: licensedLimitNearlyExceeded (133)	Severity: major Object Type (class): License Domain: security Self-clearing alarm raised: Yes	
Alarm name: Licensed7450MdaLimitExceeded Alarm ID: 259 Type: licensingAlarm (23) Probable causes: licensedLimitExceeded (106)	Severity: critical Object Type (class): License Domain: security Self-clearing alarm raised: Yes	
Alarm name: Licensed7450MdaLimitNearing Alarm ID: 257 Type: licensingAlarm (23) Probable causes: licensedLimitNearing (132)	Severity: warning Object Type (class): License Domain: security Self-clearing alarm raised: Yes	
Alarm name: Licensed7450MdaLimitNearlyExceeded Alarm ID: 258 Type: licensingAlarm (23) Probable causes: licensedLimitNearlyExceeded (133)	Severity: major Object Type (class): License Domain: security Self-clearing alarm raised: Yes	
Alarm name: LicensedCleLimitExceeded Alarm ID: 170 Type: licensingAlarm (23) Probable causes: licensedLimitExceeded (106)	Severity: critical Object Type (class): License Domain: security Self-clearing alarm raised: Yes	
Alarm name: LicensedCleLimitNearing Alarm ID: 168 Type: licensingAlarm (23) Probable causes: licensedLimitNearing (132)	Severity: warning Object Type (class): License Domain: security Self-clearing alarm raised: Yes	
Alarm name: LicensedCleLimitNearlyExceeded Alarm ID: 169 Type: licensingAlarm (23) Probable causes: licensedLimitNearlyExceeded (133)	Severity: major Object Type (class): License Domain: security Self-clearing alarm raised: Yes	

(2 of 6)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: LicensedCmaLimitExceeded Alarm ID: 236 Type: licensingAlarm (23) Probable causes: licensedLimitExceeded (106)	Severity: critical Object Type (class): License Domain: security Self-clearing alarm raised: Yes	Choose Help->5620 SAM License Information to display the 5620 SAM licence information.
Alarm name: LicensedCmaLimitNearing Alarm ID: 237 Type: licensingAlarm (23) Probable causes: licensedLimitNearing (132)	Severity: warning Object Type (class): License Domain: security Self-clearing alarm raised: Yes	
Alarm name: LicensedCmaLimitNearlyExceeded Alarm ID: 238 Type: licensingAlarm (23) Probable causes: licensedLimitNearlyExceeded (133)	Severity: major Object Type (class): License Domain: security Self-clearing alarm raised: Yes	
Alarm name: LicensedCpaaLimitExceeded Alarm ID: 389 Type: cpamLicensingAlarm (39) Probable causes: cpamLicensedLimitExceeded (285)	Severity: critical Object Type (class): CpamLicense Domain: security Self-clearing alarm raised: Yes	
Alarm name: LicensedCpaaLimitNearing Alarm ID: 390 Type: cpamLicensingAlarm (39) Probable causes: cpamLicensedLimitNearing (283)	Severity: warning Object Type (class): CpamLicense Domain: security Self-clearing alarm raised: Yes	
Alarm name: LicensedCpaaLimitNearlyExceeded Alarm ID: 391 Type: cpamLicensingAlarm (39) Probable causes: cpamLicensedLimitNearlyExceeded (284)	Severity: major Object Type (class): CpamLicense Domain: security Self-clearing alarm raised: Yes	
Alarm name: LicensedGneLimitExceeded Alarm ID: 262 Type: licensingAlarm (23) Probable causes: licensedLimitExceeded (106)	Severity: critical Object Type (class): License Domain: security Self-clearing alarm raised: Yes	
Alarm name: LicensedGneLimitNearing Alarm ID: 260 Type: licensingAlarm (23) Probable causes: licensedLimitNearing (132)	Severity: warning Object Type (class): License Domain: security Self-clearing alarm raised: Yes	
Alarm name: LicensedGneLimitNearlyExceeded Alarm ID: 261 Type: licensingAlarm (23) Probable causes: licensedLimitNearlyExceeded (133)	Severity: major Object Type (class): License Domain: security Self-clearing alarm raised: Yes	

(3 of 6)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: LicensedMdaLimitExceeded Alarm ID: 167 Type: licensingAlarm (23) Probable causes: licensedLimitExceeded (106)	Severity: critical Object Type (class): License Domain: security Self-clearing alarm raised: Yes	Choose Help->5620 SAM License Information to display the 5620 SAM licence information.
Alarm name: LicensedMdaLimitNearing Alarm ID: 165 Type: licensingAlarm (23) Probable causes: licensedLimitNearing (132)	Severity: warning Object Type (class): License Domain: security Self-clearing alarm raised: Yes	
Alarm name: LicensedMdaLimitNearlyExceeded Alarm ID: 166 Type: licensingAlarm (23) Probable causes: licensedLimitNearlyExceeded (133)	Severity: major Object Type (class): License Domain: security Self-clearing alarm raised: Yes	
Alarm name: LicensedRouterLimitExceeded Alarm ID: 348 Type: cpamLicensingAlarm (39) Probable causes: cpamLicensedLimitExceeded (285)	Severity: critical Object Type (class): CpamLicense Domain: security Self-clearing alarm raised: Yes	
Alarm name: LicensedRouterLimitNearing Alarm ID: 343 Type: cpamLicensingAlarm (39) Probable causes: cpamLicensedLimitNearing (283)	Severity: warning Object Type (class): CpamLicense Domain: security Self-clearing alarm raised: Yes	
Alarm name: LicensedRouterLimitNearlyExceeded Alarm ID: 344 Type: cpamLicensingAlarm (39) Probable causes: cpamLicensedLimitNearlyExceeded (284)	Severity: major Object Type (class): CpamLicense Domain: security Self-clearing alarm raised: Yes	
Alarm name: LicenseMismatch Alarm ID: 342 Type: licensingAlarm (23) Probable causes: licenseMismatch (247)	Severity: critical Object Type (class): License Domain: security Self-clearing alarm raised: No	
Alarm name: LicenseMissMatch Alarm ID: 349 Type: cpamLicensingAlarm (39) Probable causes: cpamLicenseMissMatch (286)	Severity: critical Object Type (class): CpamLicense Domain: security Self-clearing alarm raised: No	
Alarm name: MediationAuthenticationFailure Alarm ID: 75 Type: communicationsAlarm (4) Probable causes: unsupportedSecLevel (55), notInTimeWindow (56), unknownUserName (57), unknownEngineID (58), wrongDigest (59), decryptionError (60)	Severity: warning Object Type (class): MediationPolicy Domain: security Self-clearing alarm raised: Yes	Other possible causes for this alarm include: • authentication did not occur within the time allowed • the user name or engine ID of the managed device is unknown • the wrong digest • a decryption error

(4 of 6)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: NewSsh2ServerKeyDetected Alarm ID: 285 Type: communicationsAlarm (4) Probable causes: ssh2ServerKeyMismatch (217)	Severity: warning Object Type (class): KnownHostKey Domain: security Self-clearing alarm raised: Yes	—
Alarm name: OSSDurableClientRemoved Alarm ID: 292 Type: communicationsAlarm (4) Probable causes: maximumExceededStoredMessages (223)	Severity: variable or indeterminate Object Type (class): User Domain: security Self-clearing alarm raised: No	The alarm is raised when a durable client does not process JMS messages as quickly as the 5620 SAM generates messages. The messages are backed up on the 5620 SAM server, and when the number of messages that can be stored in the database is exceeded, the client is disconnected. When the alarm is raised, investigate the client to determine why the system is slow to process durable messages. Problems may include: • message volume is too high because JMS filters are not sufficient to lower message volume • insufficient message processing time due to system design deficiencies The alarm severity is *variable* depending on the connection status of the client. The alarm severity is critical when the client that is removed is connected. The alarm severity is minor when the removed client is not connected.

(5 of 6)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: OSSClientRemoved Alarm ID: 396 Type: communicationsAlarm (4) Probable causes: maximumExceededMessages (296)	Severity: variable or indeterminate Object Type (class): User Domain: security Self-clearing alarm raised: No	The alarm is raised when a non-durable client does not process JMS messages as quickly as the 5620 SAM generates messages. The messages are backed up on the 5620 SAM server, and when the number of messages that can be stored in memory is exceeded, the client is disconnected. When the alarm is raised, investigate the client to determine why the system is slow to process messages. Problems may include the following. • The message volume is too high because JMS filters are not sufficient to lower the message volume. • There is insufficient message processing time because of system design deficiencies. The alarm severity is *variable* depending on the connection status of the client. The alarm severity is critical when the client that is removed is connected. The alarm severity is minor when the removed client is not connected.
Alarm name: TimedLicenseExpiryNotice Alarm ID: 263 Type: licensingAlarm (23) Probable causes: timedLicenseExpiryNotice (196)	Severity: warning Object Type (class): License Domain: security Self-clearing alarm raised: No	The alarm lists the end date of the timed license.

(6 of 6)

Table 3-41 Domain: server

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: AuxiliaryServerStatus Alarm ID: 311 Type: communicationsAlarm (4) Probable causes: systemFailed (144)	Severity: critical Object Type (class): AuxiliaryServer Domain: server Self-clearing alarm raised: Yes	—

Table 3-42 Domain: service

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: AccessInterfaceDown Alarm ID: 249 Type: AccessInterfaceAlarm (32) Probable causes: interfaceDown (32)	Severity: critical Object Type (class): AccessInterface Domain: service Self-clearing alarm raised: Yes	An alarm is raised when an L2 or L3 interface operational state is down, but the administrative state of the site on which the interface resides is up.
Alarm name: FrameSizeProblem Alarm ID: 37 Type: configurationAlarm (11) Probable causes: frameSizeProblem (33)	Severity: warning Object Type (class): Service Domain: service Self-clearing alarm raised: Yes	This alarm is raised when the provisioned MTU value is greater than the actual MTU value.
Alarm name: InterfaceDown Alarm ID: 36 Type: configurationAlarm (11) Probable causes: interfaceDown (32)	Severity: major Object Type (class): RedundantInterface Domain: service Self-clearing alarm raised: Yes	—
Alarm name: SapDHCPLeaseEntriesExceeded Alarm ID: 386 Type: communicationsAlarm (4) Probable causes: sapDHCPLeaseEntriesExceeded (290)	Severity: major Object Type (class): AccessInterface Domain: service Self-clearing alarm raised: No	The alarm is generated when the number of DHCP lease-state entries on a SAP reaches the configured maximum value.
Alarm name: sapDHCPProxyServerError Alarm ID: 387 Type: communicationsAlarm (4) Probable causes: UnableProxyDHCPRequest (291)	Severity: major Object Type (class): AccessInterface Domain: service Self-clearing alarm raised: No	The alarm is generated when the 5620 SAM is unable to proxy a DHCP request.
Alarm name: ServiceCustomerInconsistent Alarm ID: 242 Type: configurationAlarm (11) Probable causes: ServiceCustomerInconsistent (175)	Severity: critical Object Type (class): Service Domain: service Self-clearing alarm raised: Yes	—
Alarm name: ServiceSiteDown Alarm ID: 97 Type: serviceAlarm (16) Probable causes: siteDown (83)	Severity: critical Object Type (class): Site Domain: service Self-clearing alarm raised: Yes	All SAPs on the site are operationally down, or the service tunnels to the site are operationally down.
Alarm name: TodSuiteAssignmentFailure Alarm ID: 312 Type: todSuiteAlarm (35) Probable causes: configConflictOrResourceFull (274)	Severity: minor Object Type (class): AccessInterface Domain: service Self-clearing alarm raised: No	The alarm is generated when a Time of Day suite cannot be assigned to an aggregation scheduler, or an L2 or L3 access interface because of a configuration conflict or a lack of resources.

(1 of 2)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: TopologyMisconfigured Alarm ID: 95 Type: configurationAlarm (11) Probable causes: topologyMisconfigured (81)	Severity: critical Object Type (class): Service Domain: service Self-clearing alarm raised: Yes	The service type for the same service ID is different on another device. Check the service SDP bindings. If the required SDP bindings are missing from the service, the alarm is raised. Because VPLSs can use spoke bindings (service sites with the save VPLS ID can have spoke bindings), the alarm does not apply. A service ID is created on the router using CLI that duplicates a service ID created using the 5620 SAM. Use the 5620 SAM topology map to to view the affected object. You can delete the new and invalid service, which also deletes the service from the managed device. When 7250 SAS and Telco VLANs are configured but the port Mode parameters of the uplink ports are not set to Network, the alarm is raised. Configure the ports correctly from the 5620 SAM navigation tree.
Alarm name: TypeMismatch Alarm ID: 96 Type: configurationAlarm (11) Probable causes: serviceSiteTypeMisconfigured (82)	Severity: critical Object Type (class): Service Domain: service Self-clearing alarm raised: Yes	The same service id used by the 5620 SAM is used for a different service on another device.

(2 of 2)

Table 3-43 Domain: sitesec

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: ManagementAccessFilterMisconfigured Alarm ID: 76 Type: configurationAlarm (11) Probable causes: invalidSourcePortIdentifier (61)	Severity: warning Object Type (class): MafEntry Domain: sitesec Self-clearing alarm raised: Yes	Management access filters are used to restrict management of the device by other nodes outside specific networks or subnetworks, or through designated ports. The filters must be configured locally. The default action denies or permits management access in the absence of a more specific management access filter match. Each entry represents a collection of filter match criteria.

Table 3-44 Domain: sonetequipment

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: BerLineSignalDegradation Alarm ID: 88 Type: communicationsAlarm (4) Probable causes: berLineSignalDegradation (74)	Severity: major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	lb2er-sd reports line signal degradation BER errors. Use the threshold command to set the error rate(s) that when exceeded determine signal degradation and signal failure. When configured, lb2er-sd alarms are raised and cleared. These alarms are not issued by default.
Alarm name: BerLineSignalFailure Alarm ID: 89 Type: communicationsAlarm (4) Probable causes: berLineSignalFailure (75)	Severity: major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	lb2er-sf reports line signal failure BER errors. Use the threshold command to set the error rate(s) that when exceeded determine signal degradation and signal failure.When configured, lb2er-sf alarms are raised and cleared. These alarms are issued by default.
Alarm name: LineAlarmIndicationSignal Alarm ID: 84 Type: communicationsAlarm (4) Probable causes: lineAlarmIndicationSignal (70)	Severity: major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	Reports line alarm indication signal LAIS errors. When configured, LAIS alarms are raised and cleared.
Alarm name: LineErrorCondition Alarm ID: 94 Type: communicationsAlarm (4) Probable causes: lineErrorCondition (80)	Severity: major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	Reports a line error condition raised by the remote as a result of b1 errors received from this node. When configured, LREI traps are raised but not cleared.
Alarm name: LineRemoteDefectIndication Alarm ID: 85 Type: communicationsAlarm (4) Probable causes: lineRemoteDefectIndication (71)	Severity: major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	Reports line remote defect indication errors. LRDIs are caused by remote LOF, LOC, LOS. When configured, LRDI alarms are raised and cleared.
Alarm name: LossOfClock Alarm ID: 83 Type: communicationsAlarm (4) Probable causes: lossOfClock (69)	Severity: major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	Reports a LOC which causes the operational state of the port to be shut down.
Alarm name: RxSectionSynchronizationError Alarm ID: 93 Type: communicationsAlarm (4) Probable causes: rxSectionSynchronizationError (79)	Severity: major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	Reports section synchronization failure as reported by the S1 byte. When configured, SS1F alarms are raised and cleared.
Alarm name: SectionB1Error Alarm ID: 87 Type: communicationsAlarm (4) Probable causes: sectionB1Error (73)	Severity: major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	Reports a b1 line error condition raised by the remote node when b1 errors are received from this node. When configured, LREI traps are raised but not cleared.

(1 of 3)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: SectionLossOfFrame Alarm ID: 90 Type: communicationsAlarm (4) Probable causes: sectionLossOfFrame (76)	Severity: major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	Reports SLOF errors. When configured, SLOF alarms are raised and cleared.
Alarm name: SectionLossOfSignal Alarm ID: 91 Type: communicationsAlarm (4) Probable causes: sectionLossOfSignal (77)	Severity: major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	Reports a SLOS error on the transmit side. When configured, SLOS alarms are raised and cleared.
Alarm name: SectionS1Failure Alarm ID: 86 Type: communicationsAlarm (4) Probable causes: sectionS1Failure (72)	Severity: major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	See the RxSectionSynchronizationError alarm in this table.
Alarm name: SonetPathAlarmIndicationSignal Alarm ID: 129 Type: communicationsAlarm (4) Probable causes: pathAlarmIndicationSignal (63)	Severity: major Object Type (class): SonetChannelMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	Reports PAIS errors. When configured, PAIS alarms are raised and cleared.
Alarm name: SonetPathB3Error Alarm ID: 132 Type: communicationsAlarm (4) Probable causes: pathB3Error (66)	Severity: major Object Type (class): SonetChannelMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	Reports a path error condition raised by the remote node when b3 errors are received from this node. When configured, PREI traps are raised but not cleared.
Alarm name: SonetPathLossOfCodegroupDelineationError Alarm ID: 248 Type: communicationsAlarm (4) Probable causes: pathLossOfCodegroupDelineationError (185)	Severity: major Object Type (class): SonetChannelMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	Reports PLOP (per tributary) errors. When configured, PLOP traps are raised but not cleared.
Alarm name: SonetPathLossOfPointer Alarm ID: 130 Type: communicationsAlarm (4) Probable causes: pathLossOfPointer (64)	Severity: major Object Type (class): SonetChannelMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	Reports PLOP (per tributary) errors. When configured, PLOP traps are raised but not cleared.
Alarm name: SonetPathPayloadMismatch Alarm ID: 133 Type: communicationsAlarm (4) Probable causes: pathPayloadMismatch (67)	Severity: major Object Type (class): SonetChannelMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	Reports a PPLM. As a result, the channel is operationally down. When configured, PPLM traps are raised but not cleared.
Alarm name: SonetPathRemoteB3Error Alarm ID: 134 Type: communicationsAlarm (4) Probable causes: pathRemoteB3Error (68)	Severity: major Object Type (class): SonetChannelMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	Reports a PREI raised by the remote node when b3 errors are received from this node. When configured, PREI traps are raised but not cleared

(2 of 3)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: SonetPathRemoteDefectIndication Alarm ID: 131 Type: communicationsAlarm (4) Probable causes: pathRemoteDefectIndication (65)	Severity: major Object Type (class): SonetChannelMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	Reports path remote defect indication errors. When configured, PAIS alarms are raised and cleared.
Alarm name: SonetPathUnequippedPathError Alarm ID: 143 Type: communicationsAlarm (4) Probable causes: pathUnequippedPathError (114)	Severity: major Object Type (class): SonetChannelMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	—
Alarm name: SonetSDHLoopback Alarm ID: 407 Type: configurationAlarm (11) Probable causes: sonetSDHLoopback (303)	Severity: warning Object Type (class): SonetPortSpecifics Domain: sonetequipment Self-clearing alarm raised: No	—
Alarm name: TxSectionSynchronizationError Alarm ID: 92 Type: communicationsAlarm (4) Probable causes: txSectionSynchronizationError (78)	Severity: major Object Type (class): SonetPortMonitorSpecifics Domain: sonetequipment Self-clearing alarm raised: Yes	Reports SS1F alarms as reported by the S1 byte. When configured, SS1F alarms are raised and cleared.

(3 of 3)

Table 3-45 Domain: srrp

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: DualMaster Alarm ID: 420 Type: configurationAlarm (11) Probable causes: dualMaster (313)	Severity: major Object Type (class): Instance Domain: srrp Self-clearing alarm raised: No	—
Alarm name: InstanceDown Alarm ID: 284 Type: configurationAlarm (11) Probable causes: instanceDown (216)	Severity: major Object Type (class): Instance Domain: srrp Self-clearing alarm raised: Yes	—
Alarm name: InstanceIdMismatch Alarm ID: 416 Type: configurationAlarm (11) Probable causes: instanceIdMismatch (309)	Severity: major Object Type (class): Instance Domain: srrp Self-clearing alarm raised: No	—
Alarm name: RedundantIfMismatch Alarm ID: 419 Type: configurationAlarm (11) Probable causes: redundantIfNotProperlyPaired (312)	Severity: major Object Type (class): Instance Domain: srrp Self-clearing alarm raised: No	—

(1 of 2)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: SapMismatch Alarm ID: 417 Type: configurationAlarm (11) Probable causes: remoteSapMismatch (310)	Severity: major Object Type (class): Instance Domain: srrp Self-clearing alarm raised: No	—
Alarm name: SapTagMismatch Alarm ID: 418 Type: configurationAlarm (11) Probable causes: remoteSyncTagMismatch (311)	Severity: major Object Type (class): Instance Domain: srrp Self-clearing alarm raised: No	—
Alarm name: SubnetMismatch Alarm ID: 415 Type: configurationAlarm (11) Probable causes: ipAddressListMismatch (308)	Severity: major Object Type (class): Instance Domain: srrp Self-clearing alarm raised: Yes	—

(2 of 2)

Table 3-46 Domain: subscrident

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: backupScriptInUse Alarm ID: 274 Type: configurationAlarm (11) Probable causes: backupInUse (206)	Severity: major Object Type (class): Policy Domain: subscrident Self-clearing alarm raised: Yes	The primary script is operationally down, but one of the other scripts is operationally up.
Alarm name: noFunctioningScript Alarm ID: 275 Type: configurationAlarm (11) Probable causes: primaryBackupDown (207)	Severity: critical Object Type (class): Policy Domain: subscrident Self-clearing alarm raised: Yes	All scripts are operationally down.
Alarm name: scriptBackupLost Alarm ID: 273 Type: configurationAlarm (11) Probable causes: backupDown (205)	Severity: warning Object Type (class): Policy Domain: subscrident Self-clearing alarm raised: Yes	The primary script URL is operationally up but a lower-priority script or URL is operationally down.

Table 3-47 Domain: svt

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: IgmpSnpgGrpDroppedLimitExceeded Alarm ID: 392 Type: SdpBindingAlarm (30) Probable causes: igmpSnpgGrpMaxNbrGrpsReached (292)	Severity: warning Object Type (class): SdpBindingIgmpSnpgCfg Domain: svt Self-clearing alarm raised: No	The alarm is generated when an IGMP group is removed from an SDP binding because a configurable maximum number of IGMP groups is reached.
Alarm name: KeepAliveProblem Alarm ID: 100 Type: oamAlarm (18) Probable causes: keepAliveFailed (86)	Severity: warning Object Type (class): Tunnel Domain: svt Self-clearing alarm raised: Yes	—
Alarm name: LabelProblem Alarm ID: 98 Type: CircuitAlarm (17) Probable causes: labelProblem (84)	Severity: critical Object Type (class): SdpBinding Domain: svt Self-clearing alarm raised: Yes	This alarm is raised when either an ingress or an egress label is missing.
Alarm name: SdpBindingDown Alarm ID: 221 Type: SdpBindingAlarm (30) Probable causes: SdpBindingNotReady (166)	Severity: critical Object Type (class): SdpBinding Domain: svt Self-clearing alarm raised: Yes	This alarm is raised when the SDP binding administrative state is up and the SDP binding operational state is not up.
Alarm name: SdpBindingMisconfigured Alarm ID: 293 Type: SdpBindingAlarm (30) Probable causes: returnSdpBindingTypeMismatch (224)	Severity: critical Object Type (class): SdpBinding Domain: svt Self-clearing alarm raised: Yes	The alarm is raised when the return SDP binding type (the circuitType) does not match the type of the originating SDP binding. For example, the alarm is raised when the return SDP binding is spoke and the originating SDP binding is mesh.
Alarm name: SdpBindingTunnelDown Alarm ID: 222 Type: CircuitAlarm (17) Probable causes: SdpTunnelNotReady (167)	Severity: critical Object Type (class): SdpBinding Domain: svt Self-clearing alarm raised: Yes	This alarm is raised when the operational state of the SDP binding is sdpNotReady (the SDP signaling session is down) or sdpDown (the SDP is not operationally up). Possible causes are: • The underlying LSP is operationally down. • The LDP sessions are down. This alarm was formerly called CircuitDown.

Table 3-48 Domain: sw

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: BootableConfigBackupFailed Alarm ID: 103 Type: configurationAlarm (11) Probable causes: fileTransferFailure (89)	Severity: major Object Type (class): BackupRestoreManager Domain: sw Self-clearing alarm raised: Yes	The 5620 SAM failed to back up the node configuration files.
Alarm name: BootableConfigRestoreFailed Alarm ID: 104 Type: configurationAlarm (11) Probable causes: fileTransferFailure (89)	Severity: major Object Type (class): BackupRestoreManager Domain: sw Self-clearing alarm raised: Yes	The 5620 SAM failed to restore the node configuration files.
Alarm name: BootEnvironmentSyncFailed Alarm ID: 101 Type: equipmentAlarm (3) Probable causes: bootEnvironmentSyncFailed (87)	Severity: critical Object Type (class): SoftwareUpgradeManager Domain: sw Self-clearing alarm raised: Yes	Synchronization of one or more system initialization files, between the active and standby SF/CPM cards failed. Refer to the *7750 SR OS System Guide* for more information.
Alarm name: ConfigFileSyncFailed Alarm ID: 102 Type: equipmentAlarm (3) Probable causes: configFileSyncFailed (88)	Severity: critical Object Type (class): SoftwareUpgradeManager Domain: sw Self-clearing alarm raised: Yes	Synchronization of the configuration file between CPM cards failed.
Alarm name: HardwareBootFailure Alarm ID: 108 Type: softwareAlarm (19) Probable causes: softwareBootProblemDueToHardwareIssues (92)	Severity: critical Object Type (class): CardSoftware Domain: sw Self-clearing alarm raised: Yes	The managed device software failed to boot because of hardware issue(s).
Alarm name: PrimaryImageBootFailure Alarm ID: 191 Type: configurationAlarm (11) Probable causes: bootOptionFileMisconfigured (150)	Severity: warning Object Type (class): CardSoftware Domain: sw Self-clearing alarm raised: Yes	—
Alarm name: SaveConfigFailed Alarm ID: 105 Type: configurationAlarm (11) Probable causes: fileAccessError (90)	Severity: major Object Type (class): BackupRestoreManager Domain: sw Self-clearing alarm raised: Yes	The admin save command failed on the managed device.
Alarm name: SoftwareBootFailure Alarm ID: 107 Type: softwareAlarm (19) Probable causes: softwareBootProblem (91)	Severity: major Object Type (class): CardSoftware Domain: sw Self-clearing alarm raised: Yes	—
Alarm name: SoftwareDownloading Alarm ID: 109 Type: softwareAlarm (19) Probable causes: softwareDownloading (93)	Severity: warning Object Type (class): CardSoftware Domain: sw Self-clearing alarm raised: Yes	—

(1 of 2)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: SoftwareInitialized Alarm ID: 111 Type: softwareAlarm (19) Probable causes: softwareInitialized (95)	Severity: warning Object Type (class): CardSoftware Domain: sw Self-clearing alarm raised: Yes	—
Alarm name: SoftwareInitializing Alarm ID: 110 Type: softwareAlarm (19) Probable causes: softwareInitializing (94)	Severity: warning Object Type (class): CardSoftware Domain: sw Self-clearing alarm raised: Yes	—
Alarm name: SoftwareUpgradeFailed Alarm ID: 106 Type: configurationAlarm (11) Probable causes: fileAccessError (90)	Severity: major Object Type (class): SoftwareUpgradeManager Domain: sw Self-clearing alarm raised: No	The software upgrade using the 5620 SAM failed.
Alarm name: StatsRetrieveFailed Alarm ID: 244 Type: configurationAlarm (11) Probable causes: fileTransferFailure (89)	Severity: major Object Type (class): AccountingStatsRetrievalManager Domain: sw Self-clearing alarm raised: No	—

(2 of 2)

Table 3-49 Domain: tdmequipment

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: DS1E1AlarmIndicationSignal Alarm ID: 112 Type: communicationsAlarm (4) Probable causes: alarmIndicationSignal (96)	Severity: major Object Type (class): DS1E1ChannelSpecifics Domain: tdmequipment Self-clearing alarm raised: Yes	—
Alarm name: DS1E1Loopback Alarm ID: 409 Type: configurationAlarm (11) Probable causes: ds1e1Loopback (305)	Severity: warning Object Type (class): DS1E1ChannelSpecifics Domain: tdmequipment Self-clearing alarm raised: No	—
Alarm name: DS1E1Looped Alarm ID: 126 Type: communicationsAlarm (4) Probable causes: farEndLoopback (102)	Severity: major Object Type (class): DS1E1ChannelSpecifics Domain: tdmequipment Self-clearing alarm raised: Yes	—
Alarm name: DS1E1LossOfSignal Alarm ID: 124 Type: communicationsAlarm (4) Probable causes: lossOfSignal (99)	Severity: major Object Type (class): DS1E1ChannelSpecifics Domain: tdmequipment Self-clearing alarm raised: Yes	—

(1 of 2)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: DS1E1OutOfFrame Alarm ID: 125 Type: communicationsAlarm (4) Probable causes: outOfFrame (100)	Severity: major Object Type (class): DS1E1ChannelSpecifics Domain: tdmequipment Self-clearing alarm raised: Yes	—
Alarm name: DS1E1ResourceAvailabilityIndicator Alarm ID: 114 Type: communicationsAlarm (4) Probable causes: resourceAvailabilityIndicator (98)	Severity: major Object Type (class): DS1E1ChannelSpecifics Domain: tdmequipment Self-clearing alarm raised: Yes	—
Alarm name: DS3E3AlarmIndicationSignal Alarm ID: 115 Type: communicationsAlarm (4) Probable causes: alarmIndicationSignal (96)	Severity: major Object Type (class): DS3E3ChannelSpecifics Domain: tdmequipment Self-clearing alarm raised: Yes	—
Alarm name: DS3E3Loopback Alarm ID: 408 Type: configurationAlarm (11) Probable causes: ds3e3Loopback (304)	Severity: warning Object Type (class): DS3E3ChannelSpecifics Domain: tdmequipment Self-clearing alarm raised: No	—
Alarm name: DS3E3Looped Alarm ID: 120 Type: communicationsAlarm (4) Probable causes: farEndLoopback (102)	Severity: major Object Type (class): DS3E3ChannelSpecifics Domain: tdmequipment Self-clearing alarm raised: Yes	—
Alarm name: DS3E3LossOfSignal Alarm ID: 116 Type: communicationsAlarm (4) Probable causes: lossOfSignal (99)	Severity: major Object Type (class): DS3E3ChannelSpecifics Domain: tdmequipment Self-clearing alarm raised: Yes	—
Alarm name: DS3E3OutOfFrame Alarm ID: 117 Type: communicationsAlarm (4) Probable causes: outOfFrame (100)	Severity: major Object Type (class): DS3E3ChannelSpecifics Domain: tdmequipment Self-clearing alarm raised: Yes	—
Alarm name: DS3E3ResourceAvailability Alarm ID: 119 Type: communicationsAlarm (4) Probable causes: resourceAvailabilityIndicator (98)	Severity: major Object Type (class): DS3E3ChannelSpecifics Domain: tdmequipment Self-clearing alarm raised: Yes	—

(2 of 2)

Table 3-50 Domain: template

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: ChildTemplateInvalid Alarm ID: 193 Type: configurationAlarm (11) Probable causes: referencedObjectInvalid (152)	Severity: major Object Type (class): TemplateBinding Domain: template Self-clearing alarm raised: Yes	—
Alarm name: DependentObjectDeleted Alarm ID: 192 Type: configurationAlarm (11) Probable causes: referencedObjectGone (151)	Severity: major Object Type (class): Template Domain: template Self-clearing alarm raised: Yes	—
Alarm name: ParentTemplateInvalid Alarm ID: 194 Type: configurationAlarm (11) Probable causes: referencedObjectInvalid (152)	Severity: major Object Type (class): TemplateBinding Domain: template Self-clearing alarm raised: Yes	—

Table 3-51 Domain: topology

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: IsisLspRateThresholdExceeded Alarm ID: 376 Type: topologyAlarm (34) Probable causes: unstableIGPNetwork (241)	Severity: major Object Type (class): Cpaa Domain: topology Self-clearing alarm raised: Yes	—
Alarm name: IsisLspThresholdExceeded Alarm ID: 375 Type: topologyAlarm (34) Probable causes: largeIGPNetwork (276)	Severity: major Object Type (class): Cpaa Domain: topology Self-clearing alarm raised: Yes	—
Alarm name: IsisReachabilityThresholdExceeded Alarm ID: 377 Type: topologyAlarm (34) Probable causes: manyExternalLSAsFloodingIntoIGP (271)	Severity: major Object Type (class): Cpaa Domain: topology Self-clearing alarm raised: Yes	—
Alarm name: ManagedRouteFailedRetryThresholdCrossed Alarm ID: 397 Type: topologyAlarm (34) Probable causes: managedRouteCouldNotBeSetup (298)	Severity: major Object Type (class): RouteManager Domain: topology Self-clearing alarm raised: Yes	—

(1 of 3)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: ManagedRouteRetryAttemptsExhausted Alarm ID: 398 Type: topologyAlarm (34) Probable causes: managedRouteCouldNotBeSetup (298)	Severity: major Object Type (class): RouteManager Domain: topology Self-clearing alarm raised: No	—
Alarm name: OspfExternalLsaThresholdExceeded Alarm ID: 372 Type: topologyAlarm (34) Probable causes: manyExternalLSAsFloodingIntoIGP (271)	Severity: major Object Type (class): Cpaa Domain: topology Self-clearing alarm raised: Yes	—
Alarm name: OspfInternalLsaRateThresholdExceededPerArea Alarm ID: 310 Type: topologyAlarm (34) Probable causes: unstableIGPNetwork (241)	Severity: major Object Type (class): Area Domain: topology Self-clearing alarm raised: Yes	—
Alarm name: OspfInternalLsaThresholdExceededPerArea Alarm ID: 309 Type: topologyAlarm (34) Probable causes: largeIgpNetwork (240)	Severity: major Object Type (class): Area Domain: topology Self-clearing alarm raised: Yes	—
Alarm name: OspfLsaRateThresholdExceededPerRouter Alarm ID: 308 Type: topologyAlarm (34) Probable causes: unstableLinksOnRouter (239)	Severity: major Object Type (class): Router Domain: topology Self-clearing alarm raised: Yes	—
Alarm name: OspfLsaThresholdExceededPerRouter Alarm ID: 374 Type: topologyAlarm (34) Probable causes: routerAdvertisingManyLSAs (273)	Severity: major Object Type (class): Router Domain: topology Self-clearing alarm raised: Yes	—
Alarm name: TooManyCpaaForIsisLevel2 Alarm ID: 384 Type: configurationAlarm (11) Probable causes: tooManyCpaaForIsisLevel2 (288)	Severity: critical Object Type (class): Cpaa Domain: topology Self-clearing alarm raised: Yes	—

(2 of 3)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: TooManyCpaaPerOspfArea Alarm ID: 383 Type: configurationAlarm (11) Probable causes: tooManyCpaaPerOspfArea (287)	Severity: critical Object Type (class): Cpaa Domain: topology Self-clearing alarm raised: Yes	—
Alarm name: TopologyIsisSystemError Alarm ID: 373 Type: topologyAlarm (34) Probable causes: isisSystemNotAdvertisingTeRouterId (272)	Severity: major Object Type (class): AutonomousSystem Domain: topology Self-clearing alarm raised: Yes	—

(3 of 3)

Table 3-52 Domain: tunnelmgmt

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: TopologyRuleExecutionError Alarm ID: 365 Type: configurationAlarm (11) Probable causes: ruleErrorOrRuleEngineError (262)	Severity: major Object Type (class): TopologyRule Domain: tunnelmgmt Self-clearing alarm raised: No	The alarm is generated when it is not possible to execute a topology rule or the rule execution generates an error. In this context, rule execution is defined as the process that determines which tunnel elements require creation, modification, or deletion. This alarm typically indicates problems with the rule configuration.
Alarm name: TunnelElementCreationError Alarm ID: 366 Type: configurationAlarm (11) Probable causes: unableToCreateTunnelElement (263)	Severity: major Object Type (class): TopologyRule Domain: tunnelmgmt Self-clearing alarm raised: No	The alarm is generated when the creation of a missing tunnel element fails.
Alarm name: TunnelElementDeleteError Alarm ID: 367 Type: configurationAlarm (11) Probable causes: tunnelElementInUse (264)	Severity: major Object Type (class): TopologyRule Domain: tunnelmgmt Self-clearing alarm raised: No	The alarm is generated when the deletion of an obsolete or unused tunnel element fails.
Alarm name: TunnelElementInUseWarning Alarm ID: 368 Type: configurationAlarm (11) Probable causes: tunnelElementInUse (264)	Severity: warning Object Type (class): TopologyRule Domain: tunnelmgmt Self-clearing alarm raised: No	The alarm is generated when the deletion of an obsolete or unused tunnel element is not attempted because the element is in use by another entity.

Table 3-53 Domain: vlan

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: IfVlanSubTypeConflict Alarm ID: 213 Type: configurationAlarm (11) Probable causes: topologyMisconfigured (81)	Severity: major Object Type (class): L2AccessInterface Domain: vlan Self-clearing alarm raised: Yes	—
Alarm name: ManagementVlanConflict Alarm ID: 215 Type: configurationAlarm (11) Probable causes: topologyMisconfigured (81)	Severity: warning Object Type (class): Vlan Domain: vlan Self-clearing alarm raised: Yes	—
Alarm name: SapVlanSubTypeConflict Alarm ID: 290 Type: configurationAlarm (11) Probable causes: topologyMisconfigured (81)	Severity: warning Object Type (class): Site Domain: vlan Self-clearing alarm raised: No	The alarm is raised when a resynchronization of a SAP indicates that its VLAN subtype is different than the subtype configured for the site. The port ID of the port associated with the SAP is shown in the alarm.
Alarm name: SiteManagementVlanConflict Alarm ID: 223 Type: configurationAlarm (11) Probable causes: topologyMisconfigured (81)	Severity: warning Object Type (class): Site Domain: vlan Self-clearing alarm raised: Yes	—
Alarm name: SiteVlanSubTypeConflict Alarm ID: 224 Type: configurationAlarm (11) Probable causes: topologyMisconfigured (81)	Severity: major Object Type (class): Site Domain: vlan Self-clearing alarm raised: Yes	—
Alarm name: VlanSubTypeConflict Alarm ID: 227 Type: configurationAlarm (11) Probable causes: topologyMisconfigured (81)	Severity: major Object Type (class): Vlan Domain: vlan Self-clearing alarm raised: Yes	—

Table 3-54 Domain: vll

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: EncapsulationTypeIncompatible Alarm ID: 250 Type: configurationAlarm (11) Probable causes: sapEncapsulationTypeIncompatible (189)	Severity: major Object Type (class): Vll Domain: vll Self-clearing alarm raised: No	The alarm is raised when two SAPs in an Ipipe VLL service are using mismatched encapsulation types.

Table 3-55 Domain: vpls

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: MFibTableSizeLimitReached Alarm ID: 190 Type: resourceAlarm (28) Probable causes: resourceLimitReached (131)	Severity: warning Object Type (class): Site Domain: vpls Self-clearing alarm raised: Yes	This alarm is raised against a VPLS site when a svcTlsMfibTableFullAlarmRaised trap is received. The alarm is cleared when a svcTlsMfibTableFullAlarmCleared trap is received.
Alarm name: MissSpokeConfiguration Alarm ID: 218 Type: configurationAlarm (11) Probable causes: missSpokeConfiguration (172)	Severity: warning Object Type (class): AbstractVpls Domain: vpls Self-clearing alarm raised: Yes	This alarm does not apply to 5620 SAM Release 4.0 and later.
Alarm name: MvrConfiguredFromVplsNotExist Alarm ID: 219 Type: configurationAlarm (11) Probable causes: MvrConfiguredFromVplsNotExist (164)	Severity: warning Object Type (class): L2AccessInterfaceMvrCfg Domain: vpls Self-clearing alarm raised: Yes	This alarm is raised when the fromVpls MVR property is set to the service ID of an MVR VPLS that does not exist. The alarm is cleared when the MVR VPLS is created.
Alarm name: MvrConfiguredProxySapNotExist Alarm ID: 220 Type: configurationAlarm (11) Probable causes: MvrConfiguredProxySapNotExist (165)	Severity: warning Object Type (class): L2AccessInterfaceMvrCfg Domain: vpls Self-clearing alarm raised: Yes	This alarm is raised when the configured proxy SAP does not exist. The alarm is cleared when the proxy SAP is created.

Table 3-56 Domain: vrrp

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: AuthFailure Alarm ID: 281 Type: authenticationAlarm (14) Probable causes: authFailure (46)	Severity: major Object Type (class): Instance Domain: vrrp Self-clearing alarm raised: No	The source IP address is indicated in the alarm.
Alarm name: InstanceDown Alarm ID: 284 Type: configurationAlarm (11) Probable causes: instanceDown (216)	Severity: major Object Type (class): Instance Domain: vrrp Self-clearing alarm raised: Yes	—
Alarm name: IPListMismatch Alarm ID: 282 Type: configurationAlarm (11) Probable causes: nonMatchingBackupAddressList (214)	Severity: warning Object Type (class): Instance Domain: vrrp Self-clearing alarm raised: Yes	—

(1 of 2)

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: mismatchBackupAddress Alarm ID: 279 Type: configurationAlarm (11) Probable causes: mismatchBackupAddress (212)	Severity: minor Object Type (class): VRInstance Domain: vrrp Self-clearing alarm raised: No	—
Alarm name: mismatchSubnets Alarm ID: 280 Type: configurationAlarm (11) Probable causes: mismatchSubnets (213)	Severity: major Object Type (class): VRInstance Domain: vrrp Self-clearing alarm raised: Yes	—
Alarm name: mismatchVrrpTypes Alarm ID: 278 Type: configurationAlarm (11) Probable causes: mismatchVrrpTypes (211)	Severity: minor Object Type (class): VRInstance Domain: vrrp Self-clearing alarm raised: Yes	—
Alarm name: MultipleOwners Alarm ID: 283 Type: configurationAlarm (11) Probable causes: multipleOwnersConfigured (215)	Severity: major Object Type (class): Instance Domain: vrrp Self-clearing alarm raised: No	—
Alarm name: VirtualRouterDown Alarm ID: 277 Type: configurationAlarm (11) Probable causes: virtualRouterDown (210)	Severity: major Object Type (class): VrrpVirtualRouter Domain: vrrp Self-clearing alarm raised: Yes	—

(2 of 2)

Table 3-57 Domain: vs

Alarm name, Alarm ID, type, and default probable cause	Default severity and object type	Additional information
Alarm name: UndefinedSchedulerReference Alarm ID: 118 Type: configurationAlarm (11) Probable causes: undefinedSchedulerReference (101)	Severity: warning Object Type (class): ServiceTypeDefinition Domain: vs Self-clearing alarm raised: Yes	The QoS and Scheduler tabs on the L2 Interface configuration form must have a queue that points to a scheduler with scheduler policy that is specified in the Scheduler tab.

4 — Troubleshooting services

4.1 5620 SAM troubleshooting support for services

This chapter documents how to troubleshoot VLL and VPLS service problems with no associated alarm conditions. See chapter 3 for information on how to troubleshoot a service with alarms.

Service assurance OAM diagnostics for troubleshooting services

The procedures in this chapter use some of the service assurance test manager OAM diagnostic tools in the workflow to troubleshoot a service. See the *5620 SAM User Guide* for descriptive information and how to use the OAM diagnostics.

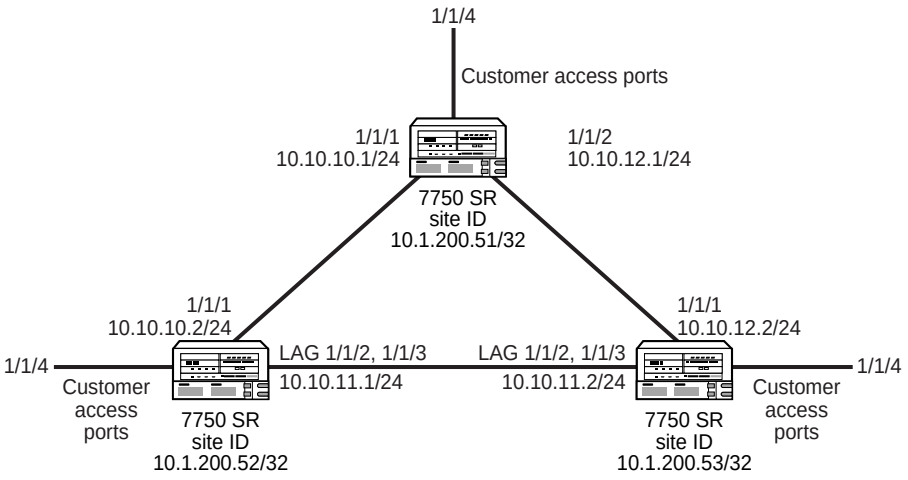
Note — You must run the OAM diagnostic tools in both directions to completely test bi-directional network objects.

The 5620 SAM service test manager (STM) provides the ability to group OAM diagnostic tests into test suites for additional fault-monitoring and troubleshooting capability. 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 and 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 sample network with 3 nodes. This example is used in the procedures that use OAM diagnostics. The configuration and results associated with the OAM diagnostics depend on the configuration of your network.

Figure 4-1 Sample network



4.2 Workflow to troubleshoot a service problem with no associated alarms

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

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

a If the MAC Ping and 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 4-5.

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 4-10.

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 4-6.

ii Verify the end-to-end connectivity on the service tunnel using the Tunnel Ping diagnostic. See Procedure 4-7.

iii Verify the end-to-end connectivity of an MPLS LSP using the LSP Ping diagnostic. See Procedure 4-8.

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 4-9.

10 Contact your Alcatel-Lucent technical support representative if the problem persists. See section 1.4 for more information.

4.3 Service troubleshooting menus

Table 4-1 lists the service troubleshooting menus and their functions.

Table 4-1 5620 SAM service troubleshooting menus

Menu option	Function
Manage→Service Tunnels	Search for and open a service tunnel, and use the OAM tools to ensure that the GRE or MPLS transport network topology is valid.
Manage→Services	Search for and open the service, site, or customer that is compromised, and use the OAM tools to troubleshoot the service.
Tools→Manage Tests	Create, edit, and manage OAM diagnostic tests

4.4 Service troubleshooting procedures

Use the following procedures to perform the service troubleshooting tasks.

Procedure 4-1 To identify if the service is part of an H-VPLS configuration

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

2 Configure the list filter parameters, 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 Services (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→Manage Tests 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.

MAC ping diagnostic information includes:

- target and source MAC addresses
- service ID and name
- number of probes to be issued
- administrative and operational states
- information about previous diagnostics
- average, minimum, and maximum round trip time values, in ms, with a value of 0 indicating no round trip measurement is available
- sum of squares round trip time for all ping responses received, used to enable a standard deviation calculation

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

Table 4-2 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.
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.

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 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 Add 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 4-6 To verify the end-to-end connectivity of a service using Service Site Ping

1 Choose Tools→Manage Tests from the 5620 SAM main menu. The Manage Tests form appears.

2 Click on the Create button.

3 Choose Service Transport→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.

Service site ping OAM diagnostic information includes:

- source and destination site IP addresses
- probes to be issued information
- check mark buttons to specify whether a local tunnel, remote tunnel, or local and remote tunnel is performed
- information about previous service site OAM diagnostics, including probes sent and responses received, loss percentage, packet timeouts, and last good packet time
- ID of the service being diagnosed

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 4-7 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 Add 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 Packets and Packet 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.

Tunnel ping OAM diagnostic information includes:

- originating and return tunnel IDs
- administrative state
- operational state
- probes to be issued information
- message size
- forwarding class used by the service
- average, minimum, and maximum one way time values, in ms, with a value of 0 indicating no one way trip measurement is available
- sum of squares one way time for all ping responses received, used to enable a standard deviation calculation
- round trip jitter, in ms, for a ping probe, with a value of 0 indicating that no measurement is available

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.

(1 of 2)

Displayed message	Description
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.

(2 of 2)

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 4-8 To verify end-to-end connectivity of an MPLS LSP using LSP Ping

1 Choose Tools→Manage Tests 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.

LSP ping diagnostics information includes:

- number of test packets to be issued
- operational size
- number of responses
- round trip jitter, in ms, for a ping probe, with a value of 0 indicating that no measurement is available
- average, minimum, and maximum one way trip time values, in ms, with a value of 0 indicating no one way trip measurement is available
- sum of squares one way trip time for all ping responses received, used to enable a standard deviation calculation

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 4-9 To review the route for an MPLS LSP using LSP Trace

1 Choose Tools→Manage Tests 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 4-10 To review the ACL filter

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 4-11 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 parameters 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 Name* (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 *Layer* 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 Find button to retrieve the current anti-spoof filters for the SAP. The Filters tab refreshes with a list of the current anti-spoof filters.

5 — Troubleshooting alarms 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

Map	Menu options
Physical view	Application→Physical Topology
Tunnel view	Application→Service Tunnel Topology
LSP view	Application→LSP Topology
Service view	Manage→Services
Composite service view	Manage→Composite Services
MPLS provisioned path view	Manage→MPLS Paths Edit an MPLS path instance, click on the Provisioned Path tab button, and click on the Topology View button for the selected item.
LSP cross-connect view	Manage→LSPs Edit an LSP instance, click on the CrossConnect tab button, and click on the Topology View button for the selected item.
LSP actual path view	Manage→LSPs Edit an LSP instance, click on the LSP Path tab. Edit an LSP path instance. Click on the Actual Path tab, .and click on the Topology View button.
LSP CSPF path view	Manage→LSPs Edit an LSP instance, click on the LSP Path tab. Edit an LSP path instance. Click on the CSPF Path tab, .and click on the Topology View button.

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

(1 of 2)

Element type	Description
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

(2 of 2)

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.
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.

(1 of 2)

Indicator	Description
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 a 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 — Troubleshooting network management LAN issues

6.1 Troubleshooting network management domain LAN issues

The following procedures describe how to troubleshoot network management domain LAN issues.

Procedure 6-1 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 6-2 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 6-3 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 6-3 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 6-4 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.

- 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.

7 — Troubleshooting Solaris and Windows platforms

7.1 Troubleshooting Solaris platforms

The following procedures describe how to troubleshoot Solaris platform workstation issues.

Procedure 7-1 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 8-1.
- Check for excess disk usage using the vmstat command, as described in Procedure 7-3.

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 7-1 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 7-1 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

(1 of 2)

Heading	Description (events per second unless noted)
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
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 7-2 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 7-3.
- Perform the 5620 SAM client GUI or OSS application procedures in chapter 8.

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 7-2 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 7-2 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 7-3 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 7-3 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 7-3 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 7-4 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 7-4 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
```

7.2 Troubleshooting Windows platforms

Many of the commands in section 7.1 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.

8 — Troubleshooting 5620 SAM clients

8.1 Troubleshooting common client application problems

The following procedures describe how to troubleshoot 5620 SAM GUI and OSS client application issues.

Procedure 8-1 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 8-2 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 8-1 lists some common printer problems.

Table 8-1 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

(1 of 2)

Problem	Probable cause	Solution
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

(2 of 2)

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 8-3 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 9-1 for more information.

Procedure 8-4 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 9-5 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 Failed Deployments tab displayed. Failed deployments are listed, and deployer, tag, state and other information is displayed. The possible states for a deployment are:

- 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 8-5 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 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.

iii Click on the Apply button to save changes, as required.

12 Click on the General tab button.

13 Verify the following parameter settings:

- Enable Backup
- Scheduled Backup Scheme
- Scheduled Backup Interval
- Scheduled Backup Sync Time
- Scheduled Backup Threshold (operations)
- Auto Backup Scheme
- Auto Backup Threshold (operations)
- CLI Config File Mode
- CLI Config Save Details
- Boot Option File Mode
- File Compression
- Auto Purge Scheme
- Number of Backups
- Maximum Backup Age (days)

14 Modify the parameters settings, if required.

15 Click on the OK button to save the changes and close the form.

Procedure 8-6 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 6 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 9-4 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 8-7 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 Review the login pop-up messages that appear when a client GUI attempts to connect to a server. Messages such as server is starting up, version mismatch between the client and server, or server is not running indicate the type of communication problem.

2 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 5620 SAM admin.

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 attributes 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.

3 To check that the 5620 SAM server is up, and to view additional server configuration information:

i Open a shell or window on the workstation on which the 5620 SAM server is installed.

ii Navigate to the 5620 SAM server installation bin directory. The default directory location is *server installation_directory*/nms/bin.

iii If the 5620 SAM server is on a PC, launch the nmsserver.bat executable with the following parameters:

```
nmsserver.bat appserver_status ↵
```

The status of the server and other server configuration information is displayed.

iv If the 5620 SAM server is on a workstation, launch the nmsserver.bash executable with the following parameters:

```
./nmsserver.bash appserver_status ↵
```

The status of the server and other server configuration information is displayed.

v To check additional server status conditions, perform Procedure 9-4.

4 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 9-1. Ensure that the license key matches the load installed. For example, you cannot use a Release 3.0 license key with 5620 SAM Release 4.0 software.

5 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. Contact your IT department to check that the local firewall is not preventing a connection to the server. The IT department can also ensure that the IP address of the 5620 SAM server is in the hosts file of the PC.

Procedure 8-8 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.

8.2 Troubleshooting client GUI issues

The following procedures describe how to troubleshoot client GUI-specific issues.

Procedure 8-9 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 Save the changes and close the form.

Procedure 8-10 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 manager, 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 8-11 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 8-12 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 9-1 for more information about viewing license keys to determine what modules are installed.

Procedure 8-13 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 8-14 Problem: Exception error message about untrusted SSL PKI certificate

When a client GUI is run after SSL is configured between the server and client GUI, an error message on the GUI or the EmsClientLog.txt file may be generated. The message in the EmsClientLog.txt file may appear like this:

```
sun.security.validator.ValidatorException: No trusted certificate
found at
sun.security.validator.SimpleValidator.buildTrustedChain(Unknown
Source) at
sun.security.validator.SimpleValidator.engineValidate(Unknown
Source) at sun.security.validator.Validator.validate(Unknown Source)
at
com.sun.net.ssl.internal.ssl.X509TrustManagerImpl.checkServerTrusted
(Unknown Source) at
com.sun.net.ssl.internal.ssl.JsseX509TrustManager.checkServerTrusted
(Unknown Source) at
com.sun.net.ssl.internal.ssl.SunJSSE_az.a(Unknown Source) at
com.sun.net.ssl.internal.ssl.SunJSSE_az.a(Unknown Source) at
com.sun.net.ssl.internal.ssl.SunJSSE_ax.a(Unknown Source) at
com.sun.net.ssl.internal.ssl.SSLSocketImpl.a(Unknown Source) at
com.sun.net.ssl.internal.ssl.SSLSocketImpl.j(Unknown Source) at
com.sun.net.ssl.internal.ssl.SSLSocketImpl.a(Unknown Source)
```

Ensure the following:

- The client GUI setenv.bat or .rc file is updated with the correct java virtual machine argument to include the path to the certificate keystore, as described in the *5620 SAM User Guide*.
- The server is properly configured to run when SSL is enabled, as described in Procedure 9-12.

Procedure 8-15 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.

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 or Linux 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 8-16 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.

9 — Troubleshooting 5620 SAM server issues

9.1 Troubleshooting 5620 SAM server issues procedures

The procedures in this chapter describe how to troubleshoot 5620 SAM server issues.

Note — 5620 SAM server performance monitoring and network statistics collection is a useful troubleshooting tool for memory-, alarm-, and SNMP-related issues on the 5620 SAM servers. See the 5620 SAM server performance and network statistics chapter in the *5620 SAM User Guide* for more information.

Procedure 9-1 Problem: Cannot manage new routers or cannot start the 5620 SAM main server

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.

i Choose Help→About 5620 SAM from the 5620 SAM client GUI main menu.

The About form opens.

ii Verify that the number of managed cards (MDAs, also called daughter cards) is not greater than the number that the license key supports. If you have a new license key with an increased number of managed cards (MDAs), you can dynamically update the license key without shutting down the server.

iii Check 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 critical alarms related to exceeding the license limits.

iv Go to the *installation_directory*/nms/config directory or folder and locate the nms-server.xml file.

v Open the nms-server.xml file using a text editor. Search on the XML tag <license>.

Contact your Alcatel-Lucent support representative to verify that your license enables the 5620 SAM-O server.

vi Type or copy-and-paste the updated license key into the file, if required, in the format:
XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-X
XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XX
XXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Include the dashes when you type the key.

vii Update the customer name, exactly as written when the license key was received.

viii Save the changes.

ix Open a shell or window.

x Go to the *installation_directory* bin directory or folder.

xi Type:

```
nmsserver.bash read_config ↵
```

The changes to the nms-server.xml file are read, and the license count for managed cards (MDAs) is updated. Any additional licensed software modules are also enabled.

2 Specific ports need to be available for the 5620 SAM server. Check the *Alcatel-Lucent 5620 SAM Planning Guide* for more information about what 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 6-4.

Procedure 9-2 Problem: A 5620 SAM server on a Solaris platform cannot be reached or does not respond

When the ping commands indicate that IP communications are 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 -s to test reachability, as described in Procedure 6-2.

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 9-3 Problem: Excessive 5620 SAM server 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 server increases. Ensure that the minimum 5620 SAM server platform requirements are met. See the *5620 SAM Planning Guide* for more information.

You can increase the available 5620 SAM server network management resources by deploying the 5620 SAM server in a distributed configuration using 5620 SAM auxiliary servers. See the *5620 SAM User Guide* and *5620 SAM System Architecture Guide* for information about 5620 SAM auxiliary server functionality. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about adding an auxiliary server to an existing 5620 SAM system.

If the 5620 SAM system includes auxiliary servers, perform this procedure to ensure that sufficient auxiliary servers are available to process requests. System performance may degrade if the number of available Preferred auxiliary servers drops below the number of configured Reserved auxiliary servers.

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 Click on the Auxiliary Servers tab button.

5 Review the list of auxiliary servers.

6 Select an auxiliary server in the list and click on the Properties button. The properties form for the auxiliary server is displayed.

7 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)

8 If the auxiliary server status is Down, perform Procedure 9-4 on the auxiliary server.

9 If the auxiliary server status is Unknown, perform Procedure 9-13 to check the connectivity between the managed network and the main and auxiliary servers.

10 Click on the Cancel button to close the System Information form.

Procedure 9-4 Problem: Unsure of the status of a 5620 SAM main or auxiliary server

A 5620 SAM main or auxiliary server startup script provides server status indicators that include the following:

- how long the server has been running
- used and available memory
- database connectivity status

1 Open a shell console window.

2 Navigate to the directory or folder that contains the 5620 SAM server startup script, for example, *installation_location*/nms/bin on a Solaris station, or *installation_location*\nms\bin on a Windows station

where *installation_location* is the folder or directory in which the 5620 SAM server is installed

3 Perform one of the following actions, depending on the type of 5620 SAM server that is being diagnosed.

a Obtain the status of a 5620 SAM main server. Run the server startup script and supply the required option. Enter the following at the command prompt:

`nmsserver.`*`file_ext option`* ↵

where
file_ext is the script file extension, for example, bash for Solaris or bat for Windows
option is one of the entries listed in Table 9-1

Table 9-1 nmsserver script options for 5620 SAM main server

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
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 polling 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

(1 of 2)

Option	Description
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)

b Obtain the status of a 5620 SAM auxiliary server. Run the server startup script and supply the required option. Enter the following at the command prompt:

```
nmsserver.bash option ↵
```

where *option* is one of the entries listed in Table 9-2

Table 9-2 nmsserver script options for 5620 SAM auxiliary server

Option	Description
auxstart	Starts the 5620 SAM auxiliary server
auxstop	Stops the 5620 SAM auxiliary server
auxappserver_status	Returns information about the operational status of the auxiliary server

(1 of 2)

Option	Description
auxstatus	Returns information about the auxiliary server that includes the following: • IP address • port number • database connections • installed server software build version
auxforce_restart	Forces the auxiliary server to restart
auxforce_stop	Forces the auxiliary server to stop
auxscript_env	Returns auxiliary server script environment information
no keyword, help, or ?	Lists the available command options

(2 of 2)

4 The following sample shows output of the nms_status option for a main 5620 SAM server. This option returns general information about the server, or about the status of the primary and standby servers in a redundant configuration. It also lists uptime information and JVM memory usage.

```
-- build info --

-- 5620 SAM Version X.X RX.0 - Built on Mon Jan XX XX:XX:XX EST
XXXX

--sys info --

-- host/IP: XXX.XXX.XXX.XXX

-- startup time: Fri Jan XX XX:XX:XX EST XXXX

-- current time: Tues Feb XX XX:XX:XX EST XXXX

-- up time: Xd XX:XX:XX.XXX

-- Java Virtual Machine memory info --

-- total memory XXX MB

-- free memory XXX MB

-- database info --

-- Primary database instance name: xxxx

... additional details including IP addresses , proxy, versions
```

```
...

-- Server Information

-- SAM Server is primary in a redundant system

... additional details including IP addresses ...

-- 5620 SAM License Information

==========================

-- Release = X.X

. . . additional details including MDA limits, CLE limits, client
limits, and whether SAM-A, SAM-E, SAM-O and SAM-P are enabled . . .
```

Procedure 9-5 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 9-6 Problem: Cannot discover more than one device or a resynchronization of devices 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 scheduling polling fails
  - slow communication and synchronization times
  - polling fails
- 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→Poller Policies from the 5620 SAM main menu. The Poller Manager (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 9-7 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 9-8 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 alarms from the 5620 SAM.

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.

Procedure 9-9 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 9-3 to ensure that system performance is not degraded because of auxiliary-server unavailability.

4 Contact your Alcatel-Lucent support representative for more information.

Procedure 9-10 Problem: Communication issues between a 5620 SAM server and database

Check the following:

- ensure that you can ping the database PC or workstation from the 5620 SAM server, as described in Procedure 9-2
- use your LAN troubleshooting procedures to ensure there are no firewall ports blocking or other LAN issues; port information is available in Procedure 6-3
- ensure that the ports specified at installation time are available

See the 5620 SAM Planning Guide for more information about the ports that must be available for 5620 SAM to function. If the problem persists, collect the logs identified in Procedure 2-1 and contact your Alcatel-Lucent support representative.

Procedure 9-11 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 interval 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 base polling interval is sufficient for the statistics you are polling in the MIB and MIB entries

Procedure 9-12 Problem: Server is unresponsive after SSL is configured

You may not be able to display the server status or stop the server when SSL is enabled.

Ensure the following:

- the server setenv.bat or .rc file is updated with the correct java virtual machine argument to include the path to the certificate keystore, as described in the *5620 SAM User Guide*
- if the server status cannot be displayed, update the execjava.bat or .bash file with the correct java virtual machine argument to include the path to the certificate keystore, as described in the *5620 SAM User Guide*
- the server is restarted after the nmsserver.bat file is updated

Use the following java virtual machine statement in the appropriate *.bat or *.rc file.

```
-Djavax.net.ssl.trustStore=samserver.keystore
```

where *samserver.keystore* is the full path to the keystore

If the keystore file is under the jboss directory, modify the *.bat or *.rc file to modify the JVM_HIGH_OPTIONS, as described in the *5620 SAM User Guide*. The following shows an example for the *.bat file.

```
set JVM_HIGH_OPTION=%JVM_OPTIONS_MEM% %JMV_OPTIONS_OTHER%

set JVM_HIGH_OPTIONS=%JVM_HIGH_OPTIONS%

-Djavax.net.ssl.trustStore=%NMS_ROOT%\nms\jboss\server\default\conf\
samserver.keystore

start "NMS client" /MIN %JRE_ROT%\bin\javaw
-Dcom.timetra.nms.propertyFile=%CONFIG_FILE% %JVM_HIGH_OPTIONS%

-Djava.security.policy=%POLICY_FILE% -classpath %CLIENT_CLASSPATH%
com.timetra.nms.client.gui.main.NmsClient
```

Procedure 9-13 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 PC or workstation, the network device management ports, and the LAN switch. This is normally done by ensuring auto-negotiation between all platforms, but in some installations the configuration may need to be forced to use a specific mode for example, 100 Mb/s half-duplex.

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.

- Are errors being reported? Errors may indicate a communication problem with the attached 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 traffic problems in only one direction.

The types of errors received determine the action to take.

- when the output shows failure errors, consider increasing the SNMP timeout value
- when the output shows 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.

When the output of step ii indicates failures, consider increasing the default SNMP timeout value, then retest to see if resynchronizations are more reliable.

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→Poller Policies menu. Click on the Mediation Security tab button.

Caution — When LAN performance is the issue, 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 set based on typical network response times

Check LAN communication issues, as specified in chapter 6. If problems persist, collect log information as specified in Procedure 2-1 and contact your Alcatel-Lucent support representative.

Procedure 9-14 Problem: The 5620 SAM server startup does not respond while trying to connect to database sessions

1 Verify network connectivity between both the primary and standby servers and the primary database by ensuring that both the primary and standby servers and the primary database can ping each other. See chapter 6 for more information.

2 Perform the following troubleshooting activities for the primary database, as described in Procedure 10-7.

- 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.

10 — Troubleshooting the 5620 SAM database

10.1 Database troubleshooting

The following procedures describe how to troubleshoot 5620 SAM database issues.

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.

Procedure 10-1 Problem: My database is running out of disk space

Sufficient database disk space is essential for your database to operate effectively. 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, as described in the *5620 SAM User Guide*, or using the 5620 SAM database installer, as described in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

6 Store the database backup in a secure location.

Procedure 10-2 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 Click on the Schedule Backup button.

4 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.

5 Modify the Backup Frequency and Frequency Unit parameters as required to improve performance.

6 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 10-3 Problem: I need to immediately restore a backed-up database to recover from a catastrophic problem

Restore the database from a backup version. If you perform the restoration of the database on the same workstation where the original database is installed, you must shut down the original database instance before performing the restore.

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.

Contact your Alcatel-Lucent technical-support representative before performing a database restore, and for assistance with performing a restore.

Procedure 10-4 Problem: I need to restore a database

A database restore may be required for a reason such as one of the following:

- the failure of the PC or workstation that houses the database
- the requirement for a rollback due to incorrect configurations in the database

This procedure is intended only to restore a database. It is not intended to upgrade a database, or create redundancy between databases on Solaris workstations. To perform upgrades or create redundancy, see the procedures in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

Before you start, ensure that:

- a regular database backup exists
- you have the release version of the database installer used to initially install and create the 5620 SAM database, and the installer version matches the version of the database being restored
- you have the database name, database instance name, and all user names and passwords used to create the database
- the database restore is done using the same Oracle instance name as the database backup
- the directory structure for the restore matches the directory structure of the database backup used for the restore

1 Determine whether you are restoring the database:

a On the same PC or workstation where the original database was installed. Go to step 2.

b On a different PC or workstation from the one on which the original database was installed. Go to step 3.

2 Remove the existing database:

i Launch the database uninstaller to remove the existing database instance and follow the prompts, as described in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

ii Restart the PC or workstation as prompted by the uninstaller.

iii Remove the remaining tablespace files in the /opt/5620sam/samdb/tablespaces or C:\5620sam\samdb\tablespace directory.

iv Remove the remaining archivelog files in the /opt/5620sam/samdb/archivelog directory or C:\5620sam\samdb\archivelog folder.

v Ensure that the orapw*database_instance_name* file is removed. Go to step 4.

3 Ensure that the database backup used for the restore has the same directory structure as the previous restore, and that the path to the backup directory on the PC or workstation where the database restore is occurring matches the backup directory on the PC or workstation where the backup was made.

4 Run the database installer, as described in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

Choose the options to specify a database restore:

- choose the restore a database from backup option
- specify the database IP address (PC or workstation IP address)
- specify the database name
- specify the database instance name
- specify the Oracle and SYS passwords, as configured during initial database installation
- specify the directory containing the backup set.
- specify whether to make a copy of the backed-up database set before restoring. The database restore process alters the backup database and renders it unusable for subsequent restores.
- specify all archivelog, tablespace, and other values as previously configured

5 Click on the Start Process button after all prompts are complete. The database restore starts. Progress is indicated in the installer window. When database restoration is complete, the installer displays a message to this effect.

6 Click on the Done button to close the database installer.

Procedure 10-5 Problem: The database restore fails with a no backupsets 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 backupsets expire based on a retention period. The default retention period is seven days. After the retention period passes, the database backupsets are set to expired. You cannot restore databases from expired backupsets.

Contact your Alcatel-Lucent technical-support representative for more information about restoring a database.

Procedure 10-6 Problem: Database redundancy is not working

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 6 for more information.

Procedure 10-7 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 6 for more information.

Procedure 10-8 Problem: Unable to verify that Oracle database and listener services are started

Oracle database and listener services are started by default on Windows PCs and Solaris workstations. If you are unsure of the status of Oracle database and listener services, perform the following.

1 Ensure that the database configuration is correct, as specified in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*

2 Perform one of the following actions.

a On Windows PCs:

i Choose Start→Settings→Control Panel→Administrative Tools→Services.

ii Scroll the list of services and verify that the Oracle*oracle_home*TNSListener, for example, OracleTNSListener, and OracleService*name_of_db* services, for example, OracleServicesamdb, show a status of started and that the startup type is Automatic.

If the service has not started, right-click on the service name from the services list and choose Start from the contextual menu. If the startup type is set to Manual instead of Automatic, right-click on the service name in the services list and choose Properties from the contextual menu. Set the Startup type to Automatic.

b On Solaris platforms, use the client GUI status bar to view the database status.

Procedure 10-9 Problem: Unable to verify status or version of the database or Oracle proxy

Oracle proxy and database services are started by default on Windows PCs and Solaris workstations. If you are not sure of the status of the installed database or the Oracle proxy, perform the following on a PC or Solaris workstation.

1 Ensure that database configuration is correct, as specified in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

2 Go to the *installation_directory*/install/config/samdb directory or folder

where *installation_directory* is the database installation directory; for example, /opt/5620sam/samdb

3 Start oracleproxy.sh or oracleproxy.bat and pass the appropriate flag as a parameter.

```
oracleproxy.* executable flag ↵
```

where
*oracleproxy.** is either oracleproxy.sh or oracleproxy.bat
executable flag is one of the options in Table 10-1

Table 10-1 oracleproxy.* flag options

Flag option	Description
start	Starts the 5620 SAM database Oracle proxy. Use of this should not be necessary, as the proxy starts by default following installation.
no flag or help	Lists available flag options.
proxy_version	Provides information about the installed proxy version.
proxy_status	Provides information about the proxy status.

(1 of 2)

Flag option	Description
db_version	Provides version information about the installed 5620 SAM database.
db_status	Provides status information about the installed 5620 SAM database.

(2 of 2)

4 The following sample shows the output of the proxy_status option.

```
Proxy is UP
```

5 The following sample shows the output of the db_version option.

```
5620 SAM Version 4.0 R1 - Build on Wed June 28 10:30:02 EST 2006
```

11 — 5620 SAM client GUI warning message output

11.1 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

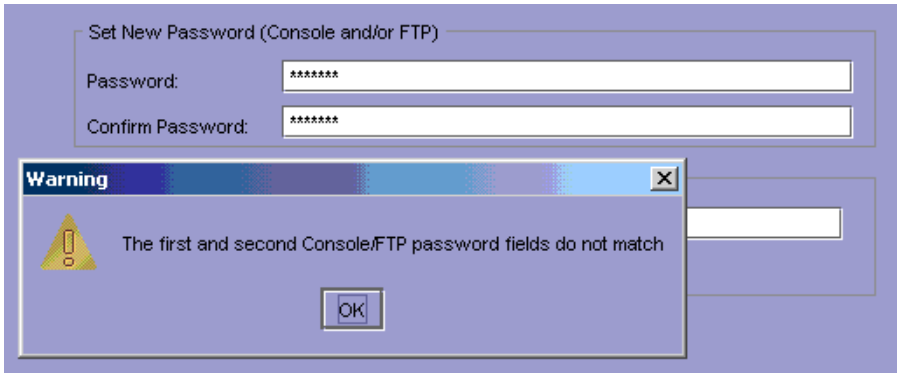
When an error condition is encountered that the 5620 SAM client has not anticipated, a Problems Encountered window is displayed. See section 12.1 for more information.

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 11-1.

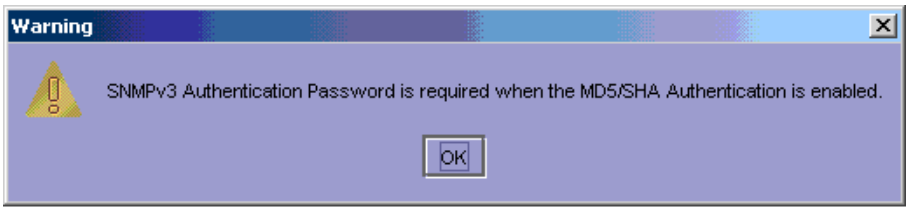
Figure 11-1 Password mismatch warning dialog box



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 11-2.

Figure 11-2 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

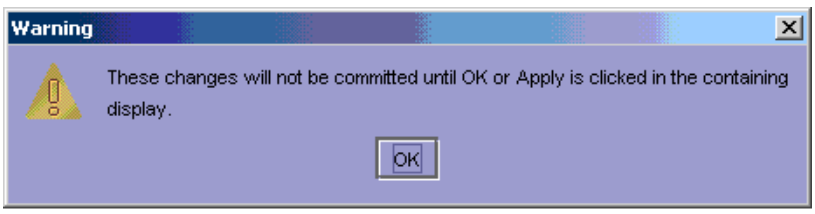
Warning messages are used to indicate that a specific action cannot be completed. These warnings may occur when you try to create a new object or modify an existing object that results in an unsupported configuration. For example, the message “Can't bind LSP to a non-mpls service tunnel“ indicates that 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

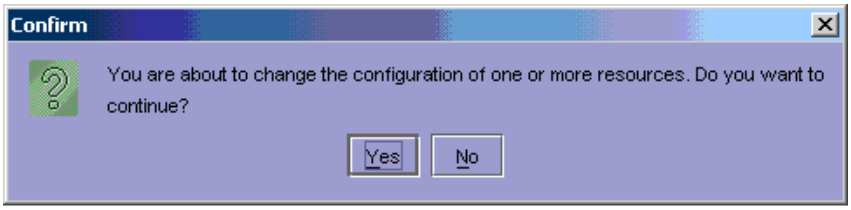
From a configuration form, you can open sub-forms that require completion before you continue with the parent form. For example, when you create a VLL service, the Create Service Site form opens during one of the configuration steps. After you configure parameters in this sub-form and click on the Finish button, a warning message is displayed, as shown in Figure 11-3.

Figure 11-3 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 11-4.

Figure 11-4 Committing changes to resources warning dialog box

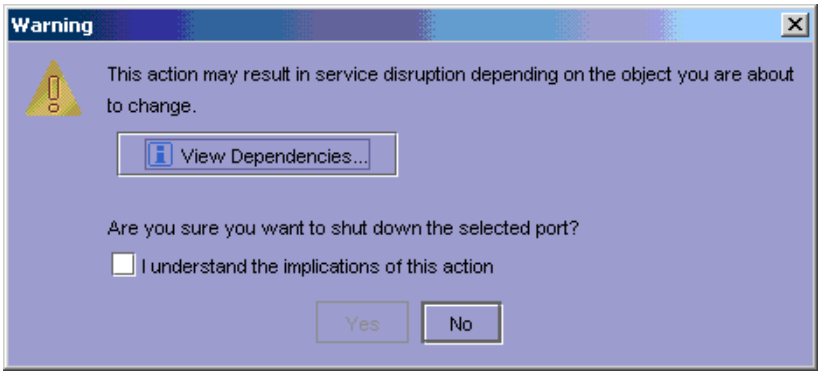


When you click on the Yes button for the last confirmation the changes to the parent or sub-forms are committed.

Service disruption warning

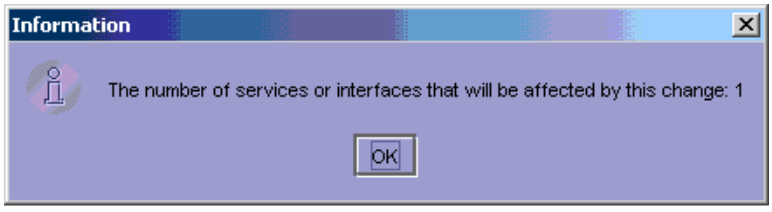
A service disruption dialog box is displayed when you perform an action that may be service-affecting. For example, if you attempt to shut down a daughter card, a warning message is displayed, as shown in Figure 11-5.

Figure 11-5 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 11-6.

Figure 11-6 View dependencies warning dialog box

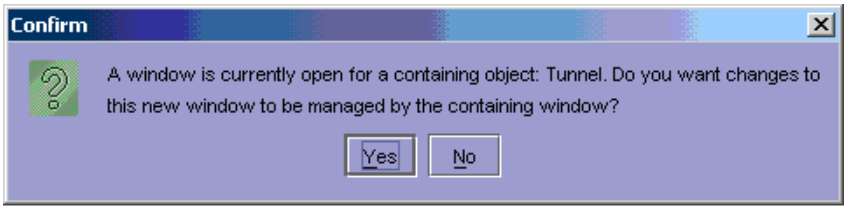


Verify that the requested action is appropriate. Click on the checkbox beside the statement “I understand the implications of this action” to continue with the action.

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 Manager form. When you try to perform both accesses, a warning message is displayed, as shown in Figure 11-7.

Figure 11-7 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.

11.2 Responding to 5620 SAM client GUI warning messages

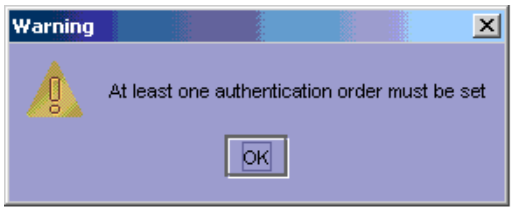
The following procedure describes how to respond to a warning message when you perform an action with the 5620 SAM client.

Procedure 11-1 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 11-8.

Figure 11-8 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 11-8, 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.

12 — Troubleshooting with Problems Encountered forms

12.1 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 12-1 shows the Problems Encountered form.

Figure 12-1 Problems Encountered form

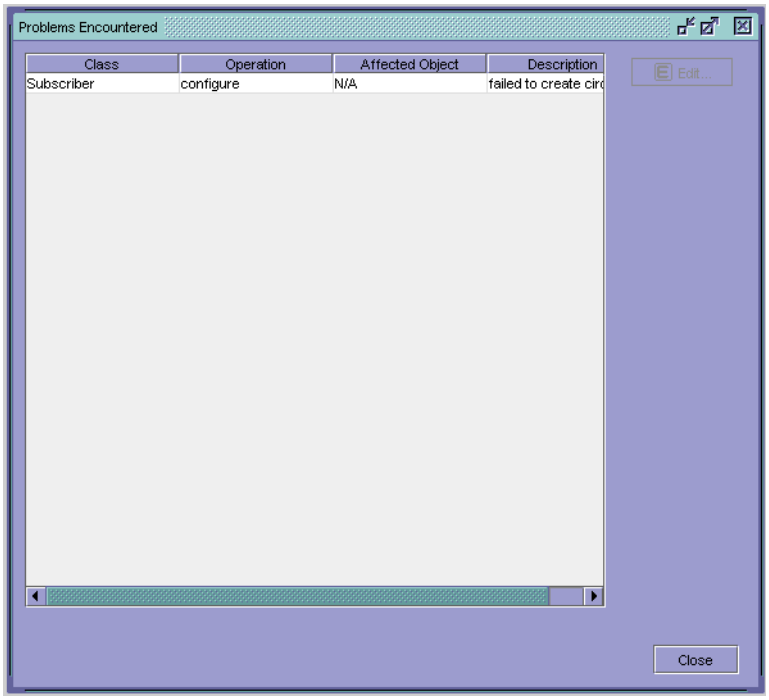


Table 12-1 describes the fields in the Problems Encountered form.

Table 12-1 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.

12.2 Using Problems Encountered forms

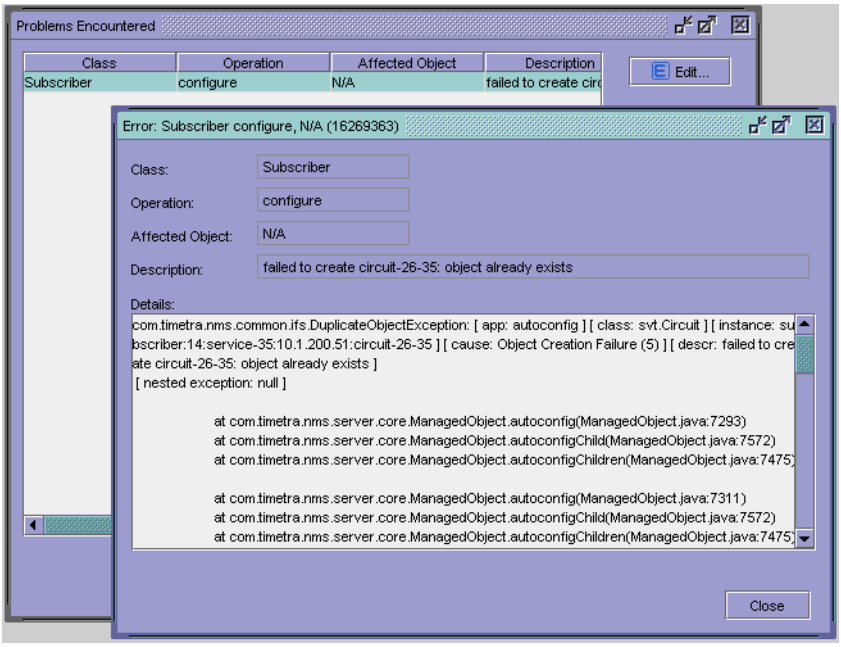
The following procedures describe how to view additional information about a problem in a Problems Encountered form and the information to collect before you contact your technical support representative.

Procedure 12-1 To view additional problem information

1 Choose an entry in the Problems Encountered form.

2 Click on the Properties button. Figure 12-2 shows a form with the problem details.

Figure 12-2 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 12-2.

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 12-2 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 12-1.
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.

13 — Troubleshooting with the client activity log

13.1 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 13-1 shows the 5620 SAM Usage and Activity Records form.

Figure 13-1 5620 SAM Usage and Activity Records form details

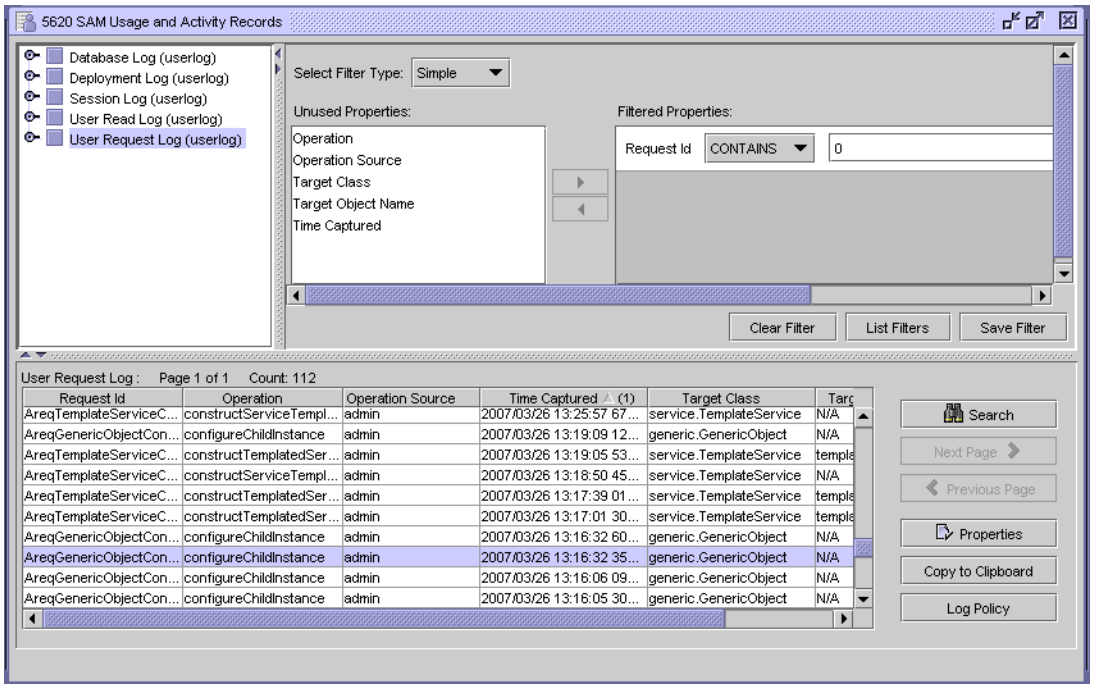


Table 13-1 describes the types of logs available in the 5620 SAM Usage and Activity Records form.

Table 13-1 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

The can also be no log entries for a client operation.

Table 13-2 lists the log file entries for select 5620 SAM actions. You must check whether logging is enabled or disabled. Logging is enabled by default for 5620 SAM, Release 4.0 or later.

Table 13-2 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.

13.2 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 13-1 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 properties 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 13-2 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 properties 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 13-3 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 properties 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 13-4 To retrieve historical user logs

1 Choose Tools→Log Records from the 5620 SAM main menu. The Manage Log Records form opens.

2 Set the Log Class parameter to the type of user log you want to view, as listed in Table 13-1.

3 Click on the Search button. A list of records appears.

4 Choose a record from the list and click on the Properties button. The logger form for the selected user log appears.

5 Click on the View History button. The Manage Log Records form reappears with the Filtered Properties panel displaying the appropriate filter.

6 Click on the Search button. A list of log records appears.

7 You can:

- **a** Click on the Time Captured column heading to sort the records chronologically.
- **b** Click on the Target Class column heading to sort the records by the type of object for the user log.
- **c** Otherwise filter or search on records and save the records to a file for post-processing purposes.
  - **i** Right-click on a column heading. The contextual menu for the list appears.
  - **ii** Filter or save the list according to user needs, as described in the *5620 SAM User Guide*.

Glossary

Numerics

5620 NM — 5620 Network Manager

The 5620 NM provides advanced management of large, complex LAN/WAN networks, including hybrid circuit-switched, IP/MPLS, ATM, frame relay, and X.25 networks. The GUI operates on a Sun workstation. It can be used to configure databases, monitor network operation in real time, set up and manage paths, and perform diagnostics to isolate and manage problems on the network.

With the addition of optional software modules, the 5620 NM can perform advanced management functions such as managing multivendor equipment, interfacing with UMS, and partitioning networks.

5620 SAM — 5620 Service Aware Manager

The 5620 SAM is the network manager portfolio of modules for the 7750 SR, 7710 SR, 7450 ESS, 7250 SAS, and Telco devices.

5620 SAM auxiliary server — In a 5620 SAM system that is deployed using distributed server architecture, a 5620 SAM server instance on a dedicated station that accepts processing requests from, and is directed by, a 5620 SAM main server. A main server and one or more auxiliary servers that are in communication are collectively called a 5620 SAM server cluster.

5620 SAM client — The 5620 SAM client provides a GUI to configure IP network elements.

5620 SAM database — The 5620 SAM database stores network data-model objects and network configuration information.

5620 SAM main server A server instance in the 5620 SAM distributed server architecture that directs one or more 5620 SAM auxiliary servers and interacts with 5620 SAM clients. The term is meaningful only in the context of a distributed 5620 SAM server deployment; the term 5620 SAM server applies to a single server instance in a non-distributed 5620 SAM deployment. A main server and one or more auxiliary servers that are in communication are collectively called a 5620 SAM server cluster.

5620 SAM server The 5620 SAM server mediates between the 5620 SAM database, the 5620 SAM client, and the network. A 5620 SAM server may be a single server instance, or, in a distributed server architecture, a server cluster that consists of one main server and one or more auxiliary servers.

5620 SAM server cluster A logical grouping in a distributed 5620 SAM server configuration that consists of a 5620 SAM main server and the 5620 SAM auxiliary servers in communication with it.

5620 SAM-A 5620 SAM Assurance

The 5620 SAM-A provides service assurance functionality.

5620 SAM-E 5620 SAM Element Manager

The 5620 SAM-E provides network element configuration and management functionality.

5620 SAM-O 5620 SAM Open Interface

The 5620 SAM-O provides an XML interface for OSS applications to interact with the 5620 SAM.

5620 SAM-P 5620 SAM Provisioning

The 5620 SAM-P provides service provisioning functionality.

7250 SAS 7250 Service Access Switch

A CE L2/L3 switch that provides VLAN, bridging, and TDM backhauling functionality and supports MPLS, Ethernet, and circuit emulation.

7450 ESS 7450 Ethernet Service Switch

The 7450 ESS is a network switch that provides scalable, high-speed Ethernet private data services with SLAs.

7710 SR 7710 Service Router

The 7710 SR is a 10-Gbyte version of the 7750 SR that provides granular lower-speed private data services with SLAs.

7750 SR 7750 Service Router

The 7750 SR is a router that provides scalable, high-speed private data services with SLAs.

A

ACL — access control list

An access control list, which is also known as a filter policy, is a template applied to services or ports to control ingress or egress network traffic on a SAP or port based on IP and MAC matching criteria. Filters are applied to services to examine packets that enter or exit a SAP or network interface. An ACL policy can be used on multiple interfaces. The same filter can be applied to ingress and egress traffic.

alarm — An alarm is a node-generated message created as a result of an event, such as an interface status change.

ANSI — American National Standards Institute

API — application programming interface

An API is a set of programming functions and routines that provides an interface to the network for application programs. APIs translate high-level program code into low-level computer instructions that run the network. Thus, application programs (for example, word processors) can communicate with low-level programs handling network data traffic.

ARP — address resolution protocol

ARP is a protocol in the TCP/IP suite that supplies a host IP address to obtain the physical address of the host, such as an Ethernet address.

auxiliary server — *See* 5620 SAM auxiliary server.

B

BGP — border gateway protocol

A BGP that supports CIDR addressing, which increases the number of available IP addresses.

BOF — boot option file

A file that specifies the runtime image, configuration files, and other operational parameters during system initialization.

C

CCAG cross-connect aggregation group

VSM-CCAs are placed in a CCAG. A CCAG provides a mechanism to aggregate multiple CCAs into one forwarding group. The CCAG uses conversation hashing to dynamically distribute cross-connect traffic to the active CCAs in the aggregation group. In the event that an active CCA fails or is removed from the group, conversation hashing redistributes the traffic over the remaining active CCAs in the group. The conversation-hashing mechanism for a CCAG is identical to that used by Ethernet LAGs.

CLE customer located equipment

CLI command line interface

The CLI is an interface that allows the user to interact with the operating system by typing alphanumeric commands and optional parameters at a command prompt. UNIX and DOS provide CLIs.

CNM customer network manager

A data integration system that takes data from the fault, performance, order management and provisioning systems of a service provider and integrates the data into a near-real-time view for the enterprise customer.

The CNM Toolkit is comprised of an Alcatel-Lucent servlet and related files that provide a simplified distributed interface to the 5620 SAM-O module. The servlet is invoked by CNM applications from a web browser.

CPM control processor module

A CPM is a module in a device such as the 7750 SR that uses hardware filters to perform traffic management and queuing functions that protect the control plane.

CPU central processing unit

The CPU is the main processing unit of a device. A CPU can be a single processor chip, a pool of processors, or a component of a multi-processor system.

CSV comma separated value

CSV is a way of recording parameters and values in text format that separates values with commas.

D

DS-N digital signal - level N

A digital signaling rate of N Mb/s; for example, the DS-1 rate is 1.544 Mb/s.

DB database

DVD digital versatile disk

An optical digital disk that stores up to 4.7 Gbytes of data. A DVD can be recorded on both sides and in dual layers.

F

fault A fault is a failure or defect in a network, causing the network, or part of the network, to malfunction.

FEC forwarding equivalency class

A group of IP packets that devices forward in the same manner, for example, over the same path, with the same forwarding treatment.

FIB forwarding information base

FIB is the set of information that represents the best forwarding information for a destination. A device derives FIB entries from the reachability information held in the RIB, which is subject to administrative routing.

FTP file transfer protocol

FTP is the Internet standard client-server protocol for transferring files from one computer to another. FTP generally runs over TCP or UDP.

G

GRE generic routing encapsulation

The encapsulation of an arbitrary network-layer protocol over another arbitrary network-layer protocol.

GUI graphical user interface

A GUI is a computer user interface that incorporates graphics to make software easier to use.

H

H-VPLS hierarchical virtual private LAN service

A type of VPLS in which access-spoke circuits interconnect with another VPLS, a VLL, or other type of service site to eliminate the need for a full mesh of virtual circuits between devices in the VPLS.

I

ID identifier or identification

IETF Internet Engineering Task Force

The IETF is the organization that provides coordination of standards and specifications that are developed for IP network and related protocols.

IOM input/output module

In the 7750 SR architecture, a circuit board that contains two independent data paths, with each path connected to an MDA. IOMs implement queuing as well as IP and MPLS functions.

IP Internet protocol

IP is the network layer for the TCP/IP protocol suite. It is a connectionless, best-effort packet-switching protocol defined by the IETF.

ISO International Standards Organization

IT information technology

J

JMS Java Message Service

JMS is an API that combines Java technology with enterprise messaging. The JMS API defines a common set of interfaces for creating applications for reliable asynchronous communication among components in a distributed computing environment, so that the applications are portable across different enterprise systems.

JVM Java Virtual Machine

A software technology developed by Sun Microsystems. Software that is developed using Java can be executed on any processor that is equipped with a JVM.

L

L1 Layer 1

The physical layer of the OSI model that includes the required network hardware and physical cabling for the transmission of raw bits and the acknowledgement of requests from the data link layer.

L2 Layer 2

The data link or MAC layer of the OSI model that includes the physical address of a client or server station for inspection by a bridge or switch.

L3 Layer 3

The network layer of the OSI model. It contains the logical address of a client or server station that is inspected by a router that forwards the address through the network. L3 contains a type field for traffic prioritization and forwarding based on the message type as well as on the network destination.

LAG link aggregation group

A LAG increases the bandwidth available between two nodes by grouping up to eight ports into one logical link. The aggregation of multiple physical links allows for load sharing and offers seamless redundancy. If one of the links fails, traffic is redistributed over the remaining links. A LAG supports up to eight links. Up to 64 LAGs can be configured on a node.

LAN local area network

A LAN is a group of computers or associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area, for example, within an office building.

LDP label distribution protocol

LDP is a signaling protocol used for MPLS path setup and teardown. An LDP is used by LSRs to indicate to other LSRs the meaning of labels used to forward traffic. LDP is defined in RFC 3036.

LLC logical link control

LLC is the upper sublayer of the ISO model data link layer. LLC governs packet transmission as specified by IEEE 802.2.

LSP label switched path

LSPs support MPLS functionality and allow network operators to perform traffic engineering. There are two types of LSPs:

- static LSP
  A static LSP specifies a static path. All devices that the LSP traverses must be configured manually with labels. No signaling is required.
- dynamic LSP
  A dynamic LSP is an LSP that is set up using a signaling protocol. The signaling protocol allows labels to be assigned from an ingress router to an egress router. Signaling is triggered by the ingress router. Only the ingress router, and not the intermediate routers, are configured. Signaling also facilitates path selection.

LSP path A LSP associated with an MPLS path. This path could be an actual route, or a configured route. A configured route can be primary, secondary, or standby. An LSP can have at most one actual route, one primary route, and multiple standby or secondary routes.

M

MAC media access control

MAC is a sublayer of the data link layer, defined in IEEE 802.2 specifications that accesses the LAN medium. The MAC layer handles the recognition and identification of individual network devices. Every computer and network node has a MAC address that is encoded in hardware.

main server *See* 5620 SAM main server.

MD5 message digest 5

MD5 is a security algorithm that takes an input message of arbitrary length and produces as an output a 128-bit message digest of the input. MD5 is intended for digital signature applications, for which a large file must be securely compressed before being encrypted.

MDA media dependent adapter

An MDA is a pluggable interface module that distributes traffic between the network and the system IOM. It is also referred to as a daughter card.

MIB management information base

A formal description of a set of network objects that can be managed using SNMP.

MPLS multiprotocol label switching

MPLS is a technology in which forwarding decisions are based on fixed-length labels inserted between the data link layer and network layer headers to increase forwarding performance and flexibility in path selection.

MTU maximum transmission unit

MTU is the largest unit of data that can be transmitted over a particular interface type in one packet. The MTU can change over a network.

N

navigation tree The navigation tree displays a view of all managed equipment, services, and protocols, and allows you to navigate through these components.

NE network element

A physical device in a network, such as a 7750 SR, or a switch, such as the 7670 RSP.

network topology A network topology is the layout of a network, which can include the way in which elements in a network, such as nodes, are connected and how they communicate.

NMS network management system

A system that manages at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer such as an engineering workstation. The NMS communicates with agents to help keep track of network statistics and resources.

NOC network operations center

Part of telecom architecture that is used to configure and monitor the network and service elements.

NTP network time protocol

An Internet protocol that network devices use to synchronize their clocks.

O

OAM operations, administration, and maintenance

A general term used to describe the costs, tasks involved, or other aspects of operating, administering, and managing a telecommunications network. The 5620 SAM provides a series of OAM tools to monitor and administer the network.

OS operating system

OSPF open shortest path first

OSPF is an IETF standard link-state routing protocol that is used to determine the most direct path for a transmission in IP networks.

OSS operations support system

A network management system supporting a specific management function, such as alarm surveillance and provisioning, in a service provider network.

P

PC personal computer

PDU protocol data unit

A PDU is a message of a given protocol comprising payload and protocol-specific control information, typically contained in a header. PDUs pass over the protocol interfaces which exist between the layers of protocols, as indicated in the OSI model.

PE provider edge

A descriptor for a device or a set of devices at the edge of the provider network with the functionality that is needed to interface with the customer and the MPLS network. A PE can be a router or a switch. All the MPLS tunnels are set up and terminated in the PE. All VPN functionalities reside in the PE.

PIM protocol independent multicast

Multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. PIM is unicast routing protocol independent and can be operated in two modes—dense and sparse.

PKI public key infrastructure

PKI represents the set of hardware, software, people, policies and procedures that are required for the creation, management, storage, distribution, and revocation of public key certificates based on public-key cryptography.

Q

QoS quality of service

QoS is a term for the set of parameters and their values that determine the performance of a virtual circuit. A service level is typically described in terms of network delay, bandwidth, and jitter.

R

RAM random access memory

A group of memory chips that function as the primary workspace of the computer. Each byte of storage in the chip can be directly accessed without regard to the bytes before or after it.

router A router is an interface device between two networks, connecting LANs to LANs or LANs to WANs. It selects the most cost-effective route for moving data between multiprotocol LANs, making sure that only one route exists between source and destination devices. Routers make forwarding decisions based on network layer addresses.

RSVP resource reservation protocol is used two ways:

1 RSVP is the process of reserving network and host resources to achieve a QoS for an application.

2 RSVP is an IP-based protocol that is used for communicating application QoS requirements to intermediate transit nodes in a network. RSVP uses a soft-state mechanism to maintain path and reservation-state information on each node in the reservation path.

S

SAP service access point

A SAP is a point of communication exchange between an application and the LLC or between layers of software.

SDP service distribution path

The 5620 SAM uses this term interchangeably with service tunnel.

service-level agreement *See* SLA.

SLA service-level agreement

An SLA is a service contract between a network service provider and a customer that guarantees a particular QoS. SLAs are used for providing network availability and data-delivery reliability.

SNMP simple network management protocol

A protocol used for the transport of network management information between a network manager and a network element. SNMP is the most commonly used standard for interworking devices.

SNMP trap An SNMP trap is an unsolicited notification that indicates that the SNMP agent on the node has detected a node event, and that the network management domain should be aware of the event. SNMP trap information typically includes alarm and status information, and standard SNMP messages.

Solaris The name for the UNIX operating system variant developed by SUN Microsystems.

SONET synchronous optical network

SONET is an ANSI standard for fiber optic transmission of high-speed digital traffic. SONET allows internetworking of transmission products from multiple vendors and defines a physical interface, optical line rates known as OC signals, frame format, and an OAM protocol. The base rate is 51.84 Mb/s (OC-1), and higher rates are multiples of the base rate.

SONET uses synchronous high-speed signals and provides easy access to low-speed signals by mapping them into VTs.

SONET is a North American standard that is technically consistent with SDH, which is international.

spoofing A technique used to gain unauthorized access to devices, whereby the intruder sends messages to a device with an IP address indicating that the message is coming from a trusted host.

SSH secure shell

The SSH protocol is used to protect communications between two hosts by encrypting a Telnet or FTP connection between the 5620 SAM and some nodes. 5620 SAM uses SSH version 1.5. Both ends of the client/server connection are authenticated, and passwords are protected by being encrypted.

T

TAC technical assistance center

The front end, or customer-facing product support structure in which the first- and second-level support reside.

TCP transmission control protocol

TCP is a protocol used, along with the Internet Protocol (IP), to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

TDM time division multiplexing

Multiplexing in which a separate periodic time interval is allocated to each tributary channel in a common aggregated channel.

telco telephone company

A company that provides local, or local and long distance telephone services.

Telnet Telnet is a part of the TCP/IP protocol suite that provides remote terminal connection service. It allows a user at one site to interact with a remote time-sharing system at another site as though the user terminal connects directly to the remote machine.

The Telnet command and program are used to log in from one Internet site to another. It displays the login prompt of another host.

TLS transparent LAN service

TLS is used to transport customer VLANs while keeping traffic in each VLAN secure from other customer VLANs. In 7250 SAS and Telco devices, TLS is a tagging mechanism in the encapsulated source Ethernet frames that are transported from the customer edge, across the provider network, to the destination customer edge.

TLV type length value

Traffic engineering information specifies the type, length, and values of the traffic engineering information that signaling objects, for example, LDPs, carry.

U

UDP user datagram protocol

A minimal transport protocol above the IP network layer that does not guarantee datagram delivery. UDP is for applications that do not require the level of service that TCP provides or that need to use communications services, such as multicast or broadcast delivery that are not available in TCP.

UNIX UNIX is a multi-user, multitasking operating system on mainframes, workstations, and PCs. UNIX is the basis of Solaris and SunOS, which are the operating systems that Sun workstations use.

V

VC virtual connection

A technique that ensures that a network delivers packets to the correct recipient in the same order as during submission.

VLL virtual leased line

A VLL is a type of VPN in which IP is transported in a point-to-point manner. CPE devices connect through nodes that connect to an IP tunnel.

VPLS virtual private LAN service

A VPLS is a type of VPN in which a number of sites are connected in a single bridged domain over an IP/MPLS network. Although the services may be from different locations, in a VPLS, they appear to be on the same LAN.

VPN virtual private network

A private network within a public network that takes advantage of the economies of scale and management of large networks. VPNs are used by enterprises to create WANs that span large geographic areas, to provide a site-to-site connection between branch offices, and to allow mobile users to dial up their company LANs.

When implemented with Layer 2 interfaces, this service is called VPLS. When implemented with Layer 3 interfaces, this service is called an IP-VPN

W

WAN wide-area network

A geographically dispersed, long-haul telecommunications network that usually consists of backbone links. A WAN may be privately owned or leased. The term usually connotes the inclusion of public networks that are highly regulated, and provide superior reliability and resilience.

window Windows are forms, panels of information, equipment drawings, or graphics that appear on a screen. Windows commonly allow a user to input data and initiate functions but some windows simply display information.

workflow The 5620 SAM workflow is a defined series of tasks that describe how to install, configure, create, and manage services.

X

X.733 ITU-T X.733

X.733 is the standard that describes the alarm reporting function.

XML extensible markup language

XML defines the syntax to customize markup languages. The markup languages are used to create, manage, and transmit documents across the Web.

Index

Numbers

A

I

J

L

M

N

O

P

R

S

T

U

V

W

Customer documentation and product support

Customer documentation

http://www.alcatel-lucent.com/osds

Product manuals and documentation updates are available through the Alcatel-Lucent Support Documentation and Software Download service 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://www.alcatel-lucent.com/support

Customer documentation feedback

documentation.feedback@alcatel-lucent.com

3HE 02241 AAAE Ed. 01