Alcatel 5620

SERVICE AWARE MANAGER | RELEASE 2.1

TROUBLESHOOTING GUIDE

ALCATEL

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

Disclaimers

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

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

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

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

PRINTED ON
RECYCLED PAPER

Alcatel License Agreement

SAMPLE END USER LICENSE AGREEMENT

1. LICENSE

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

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

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

2. PROTECTION AND SECURITY OF LICENSED PROGRAMS

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

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

3. TERM

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

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

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

4. CHARGES

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

5. SUPPORT AND UPGRADES

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

6. WARRANTIES AND INDEMNIFICATION

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

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

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

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

7. LIMITATION OF LIABILITY

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

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

8. GENERAL

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

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

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

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

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

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

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

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

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

8.10This 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 many documents that define the 5620 SAM and the managed devices.

- Contact your Alcatel support representative for more information about network sizing and recommended hardware configurations. Use the *5620 SAM Planning Guide* for more information about sizing.
- Use the *5620 SAM Installation and Upgrade Guide* to install the 5620 SAM database, server, and client software.
- Use the *5620 SAM User Guide* for information about using the client GUI to perform network management functions.
- Use the *5620 SAM Parameter Guide* for definitions, ranges, dependencies, and defaults for configurable parameters from the 5620 SAM client GUI.
- Use the *Alcatel 5620 SAM-O OSS Interface Developer Guide* for information about using the XML OSS interface to create OSS applications, such as alarm monitoring and inventory controls.
- Use the *5620 SAM Routine Maintenance Procedures Guide* to help develop and schedule regular maintenance activities.
- See the index file in the User Documentation directory on the application DVD for additional documentation.

See the 7750 SR, 7450 ESS, or Telco T5C user documentation guides for more detailed information about specific CLI commands, device installation, and additional parameter information.

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→Alarm Policies

Procedures with options or substeps

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

Example of options in a procedure

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

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

- **a** This is one option.
- **b** This is another option.

2 You must perform this step.

Example of substeps in a procedure

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

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

- **i** This is the first substep.
- **ii** This is the second substep.
- **iii** This is the third substep.

2 You must perform this step.

Important information

The following conventions are used to indicate important information:

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

Troubleshooting overview

Network troubleshooting

Network management troubleshooting

10 — Troubleshooting the 5620 SAM database 10-1

11 — 5620 SAM client GUI warning message output 11-1

12 — Troubleshooting with Problems Encountered forms 12-1

13 — Troubleshooting with the client activity log 13-1

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 section 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 router 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 that router. 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
- core dumps
- serial line traces
- stack dumps
- 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?
- Is there a change in the network delta 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 route 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 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 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 documentation and your company policies and procedures nearby.
- Check the appropriate release notice from the Support Documentation Service at www.alcatel.com 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 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 support contacts is available from the Alcatel home page at www.alcatel.com. Click on the Support link.

Table 1-1 Troubleshooting data collection for support

Action	Collect the following
Collect software and platform information	• release version and load of 5620 SAM software • Solaris, Linux, or Windows operating system version and patch set • platform information, including CPU, disk, and RAM data
Collect any applicable software logs	• The appropriate log files from the PC or workstation where the problem occurred. For example, for problems from a server, retrieve the EmsServerLog.txt file from the *install directory* log directory or folder. 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

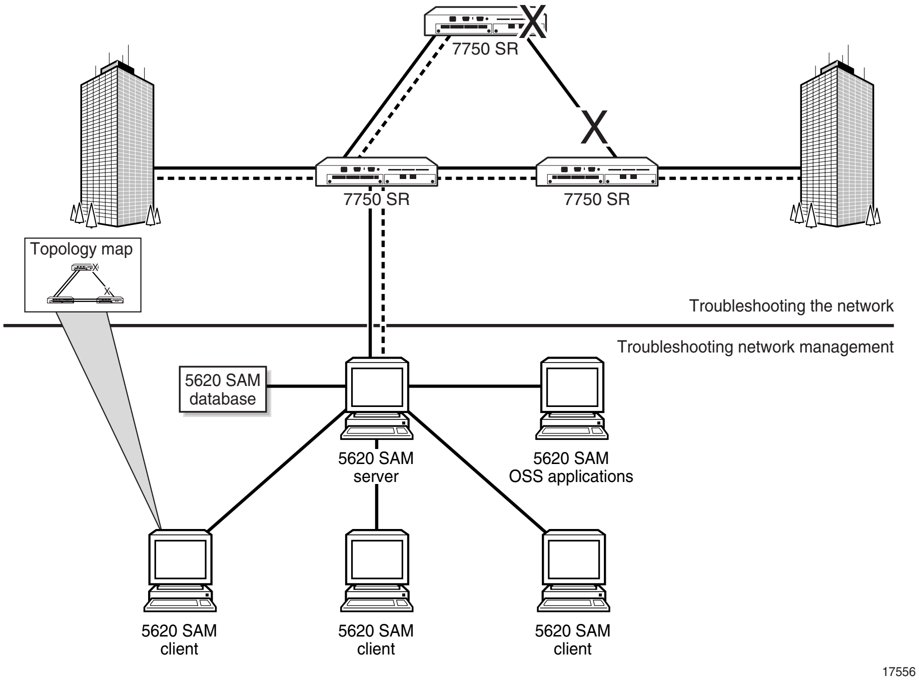
2.1 5620 SAM troubleshooting process

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 subscriber 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 to subscribers 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 and 5620 SAM-O servers, and 5620 SAM client software
- Windows, Solaris, and Linux operating systems
- PC and workstation platforms
- TCP/IP networking

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 “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 problems during 5620 SAM installation:

- stderr and stdout data 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 Collect the following files before you reboot or restart 5620 SAM software during troubleshooting:

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

b To troubleshoot the 5620 SAM or 5620 SAM-O server, collect the nms-server.xml file from the *install directory*/nms/config directory or folder.

c To troubleshoot the 5620 SAM client, collect the nms-client.xml file from the *install directory*/nms/config directory or folder.

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

e Collect server and client logs, for example, the EmsServerLog, from the *install 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 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, do not place the two nms-client.xml files in the same directory because one of them will be overwritten. Rename the files, as appropriate, to identify each 5620 SAM client.

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

ii Section 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 networkstations are experiencing performance degradation	Procedure 6-1
Problem: Garbled text when connecting using a modem from a Solaris platform	Procedure 6-2
Problem: Lost connectivity to one or more network management domain PCs or workstations	Procedure 6-3
Problem: Another machine can be pinged, but some functions are unavailable	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: Performance is slow across the clients	Procedure 8-1
Problem: Unable to print from a Solaris platform client	Procedure 8-2
Problem: I discovered a new router, but cannot place it in a 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: I cannot find the backups of the router databases	Procedure 8-5
Problem: Cannot communicate with the 5620 SAM server	Procedure 8-6
Problem: Cannot start the client, or I get an error message when I start the client	Procedure 8-7
Problem: Problem collecting large numbers of logged statistics records or other large queries	Procedure 8-8
Problem: Cannot view alarms from a 5620 SAM on a 5620 NM or 1354 BM	Procedure 8-9

(1 of 3)

Problem	Solution
Problem: The GUI keeps shutting down	Procedure 8-10
Problem: I saved a configuration on the GUI, but cannot see the change	Procedure 8-11
Problem: I performed a search or list function, and it takes too long to complete	Procedure 8-12
Problem: I cannot select certain menu options or I cannot save configurations	Procedure 8-13
Problem: I cannot see related object information for an alarm	Procedure 8-14
Problem: I cannot clear alarms using the 5620 SAM client GUI	Procedure 8-15
Problem: Received an exception that an SSL PKI certificate is not trusted	Procedure 8-16
Troubleshooting 5620 SAM server issues	
Problem: Cannot manage new routers or cannot launch the 5620 SAM server	Procedure 9-1
Problem: The 5620 SAM server on a Solaris platform cannot be reached or does not respond	Procedure 9-2
Problem: 5620 SAM server response times are slower than normal	Procedure 9-3
Problem: Unsure of the status of my server	Procedure 9-4
Problem: All SNMP traps from 7750 SRs 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: The 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: Communication issues between the 5620 SAM server and database	Procedure 9-9
Problem: Statistics are rolling over too quickly	Procedure 9-10
Problem: Redundancy issues for the 5620 SAM server and database	Procedure 9-11
Problem: server is unresponsive after SSL is configured	Procedure 9-12
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: The Oracle database is not performing as expected on a Solaris platform	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: unable to verify that Oracle database and Listener services have started	Procedure 10-7
Troubleshoot using the GUI warning messages	
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 support	Procedure 12-2
Troubleshoot with the client activity log	

(2 of 3)

Problem	Solution
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 Use the dynamic alarm list to view and monitor network alarms. See Procedure 3-1.

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

3 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 3-2.

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

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

- **i** dynamic alarm list and Alarm Info forms
- **ii** managed object hierarchy table
- **iii** alarm description tables

6 View the affected object states information. See Procedure 3-4.

7 If there is an equipment down alarm, use the navigation tree equipment view for more information and check the physical connections to the port. See Procedure 3-7.

8 View related object information if the root cause is not found on the affected object. See Procedure 3-5.

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

3.3 Troubleshooting using network alarm procedures

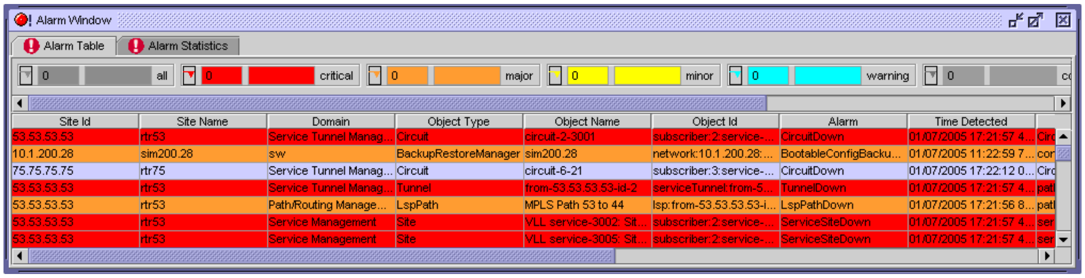
Use the following procedures to troubleshoot network problems using alarms.

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



Site Id	Site Name	Domain	Object Type	Object Name	Object Id	Alarm	Time Detected	
53.53.53.53	rtr53	Service Tunnel Manag...	Circuit	circuit-2-3001	subscriber:2:service-...	CircuitDown	01/07/2005 17:21:57 4...	Circ
10.1.200.28	sim200.28	sw	BackupRestoreManager	sim200.28	network:10.1.200.28:...	BootableConfigBacku...	01/07/2005 11:22:59 7...	cor
75.75.75.75	rtr75	Service Tunnel Manag...	Circuit	circuit-6-21	subscriber:3:service-...	CircuitDown	01/07/2005 17:22:12 0...	Circ
53.53.53.53	rtr53	Service Tunnel Manag...	Tunnel	from-53.53.53.53-id-2	serviceTunnel:from-5...	TunnelDown	01/07/2005 17:21:57 4...	patl
53.53.53.53	rtr53	Path/Routing Manage...	LspPath	MPLS Path 53 to 44	lsp:from-53.53.53.53-i...	LspPathDown	01/07/2005 17:21:56 8...	patl
53.53.53.53	rtr53	Service Management	Site	VLL service-3002: Sit...	subscriber:2:service-...	ServiceSiteDown	01/07/2005 17:21:57 4...	ser
53.53.53.53	rtr53	Service Management	Site	VLL service-3005: Sit...	subscriber:2:service-...	ServiceSiteDown	01/07/2005 17:21:57 4...	ser

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

Multiple alarms received at approximately the same time indicate that the alarms are 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 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 necessary, 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 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	For alarm information see
1	Network Element	Network (netw) alarms	Table 3-13
2	Service	Service management (svc)	Table 3-23
3	Circuit	Service tunnel management (svt)	Table 3-24
4	Tunnel	Service tunnel management (svt) Path routing management: MPLS alarms	Table 3-24 for Service tunnel management Table 3-14 for Path Routing Management: MPLS
5	dynamic LSP	Path routing management: MPLS alarms	Table 3-14
6	LSP Path		
7	Session	Routing management: RSVP	Table 3-21
8	Interface or Targeted pair for LDP	LDP	Table 3-11
9	Interface routing management	Routing Management	Table 3-20 for RIP Table 3-6 for IGMP Table 3-19 for PIM Table 3-16 for BPG Table 3-18 for OSPF Table 3-17 for ISIS
10	Network interface	Routing Management: general	—
11	Physical port and other equipment	Equipment	Table 3-4
12	Sonet port/channel Bundle	SONET Equipment Bundle	Table 3-28 for SONET Equipment Table 3-2 for Bundle
13	DS1E1 channel	TDM equipment	Table 3-29
—	Other	Alarms for other objects	Table 3-26 for SNMP domain Table 3-25 for site security Table 3-22 for security domain Table 3-27 for software domain Table 3-30 for templates Table 3-31 for virtual scheduler domain

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 3-3 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 will ensure 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.

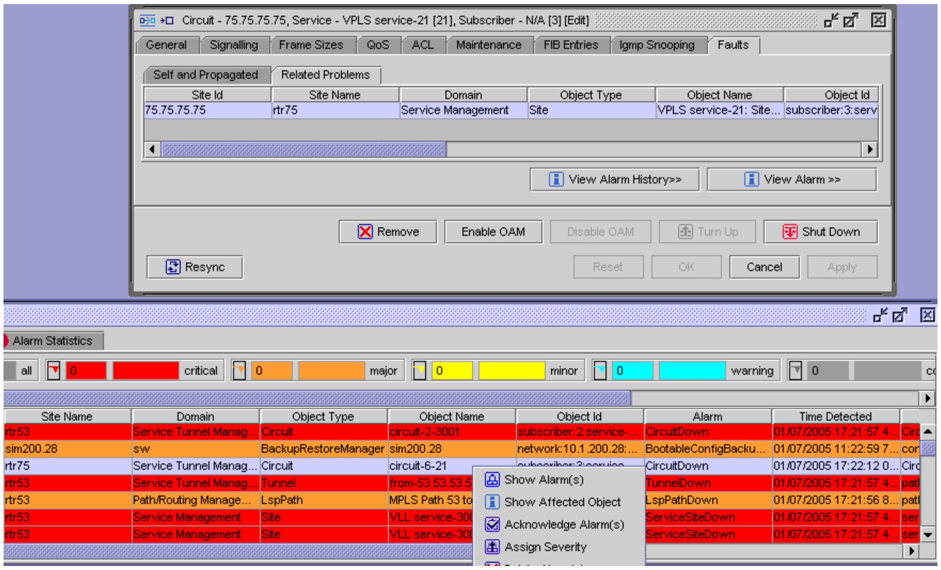
iii Click on the OK button to continue. A check mark appears for the selected alarm under the Ack. column in the dynamic alarm list.

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 Affected Object properties form opens in the working pane to the right of the navigation tree.

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

Figure 3-2 Acknowledge related problems



Site Id	Site Name	Domain	Object Type	Object Name	Object Id
75.75.75.75	rtr75	Service Management	Site	VPLS service-21: Site...	subscriber:3:serv

Site Name	Domain	Object Type	Object Name	Object Id	Alarm	Time Detected	
rtr53	Service Tunnel Manag...	Circuit	circuit-2-3001	subscriber:2:service-...	CircuitDown	01/07/2005 17:21:57 4...	Circ
sim200.28	sw	BackupRestoreManager	sim200.28	network:10.1.200.28:...	BootableConfigBacku...	01/07/2005 11:22:59 7...	cor
rtr75	Service Tunnel Manag...	Circuit	circuit-6-21	subscriber:3:service	CircuitDown	01/07/2005 17:22:12 0...	Circ
rtr53	Service Tunnel Manag...	Tunnel	from-53.53.53.5		TunnelDown	01/07/2005 17:21:57 4...	patl
rtr53	Path/Routing Manage...	LspPath	MPLS Path 53 to		LspPathDown	01/07/2005 17:21:56 8...	patl
rtr53	Service Management	Site	VLL service-30		ServiceSiteDown	01/07/2005 17:21:57 4...	ser
rtr53	Service Management	Site	VLL service-30		ServiceSiteDown	01/07/2005 17:21:57 4...	ser

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

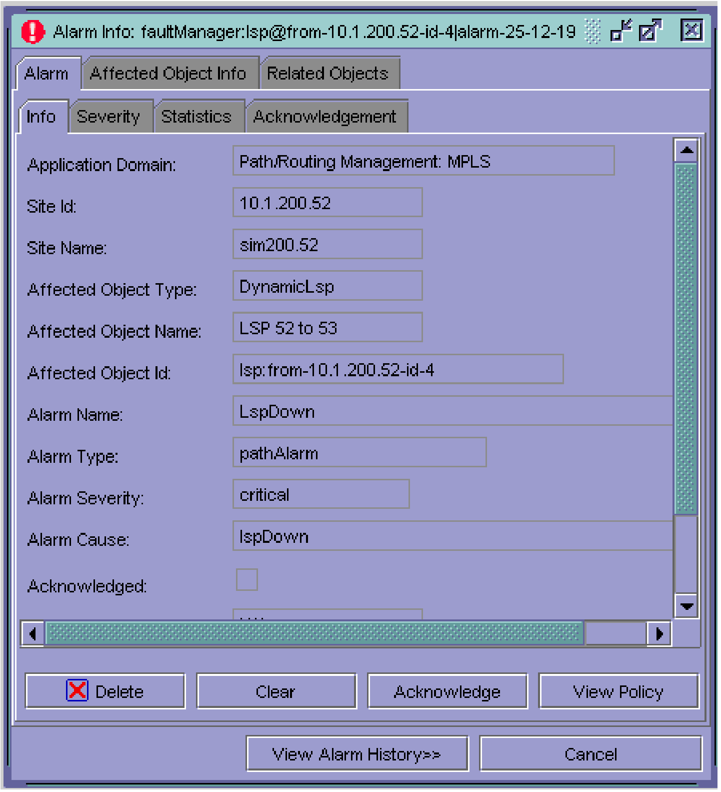
vi Click on the OK button to continue. A check mark appears for each of the selected alarms under the Ack. column in the dynamic alarm list.

Procedure 3-4 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



Application Domain:	Path/Routing Management: MPLS
Site Id:	10.1.200.52
Site Name:	sim200.52
Affected Object Type:	DynamicLsp
Affected Object Name:	LSP 52 to 53
Affected Object Id:	lsp:from-10.1.200.52-id-4
Alarm Name:	LspDown
Alarm Type:	pathAlarm
Alarm Severity:	critical
Alarm Cause:	lspDown
Acknowledged:	□

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 Object Info tab button, then click on the View Affected 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 3-5 to review related object information.

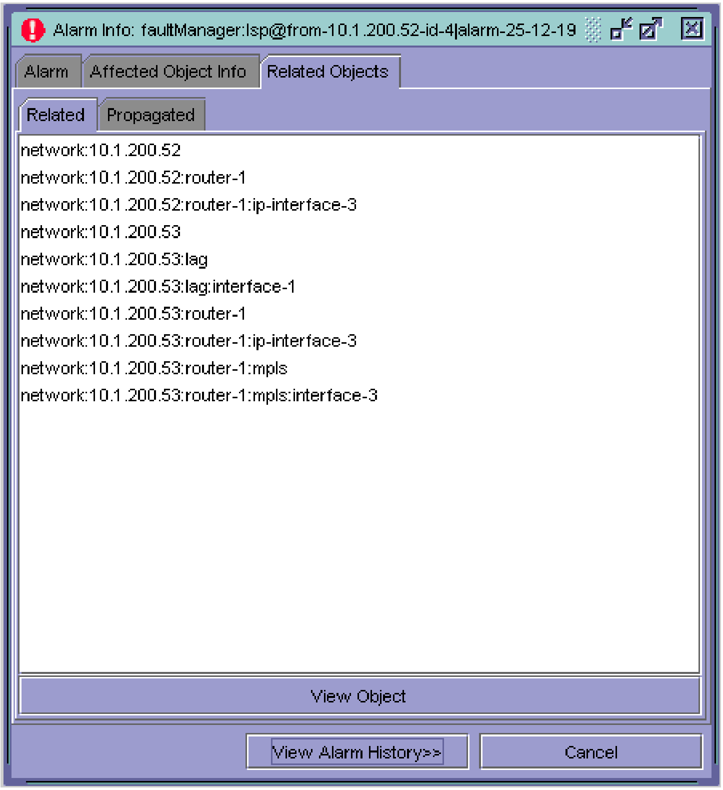
b If the Administrative State is Up and the Operational State is not Up or Down but states a specific problem such as Not Ready or MTU Mismatch, this is the root cause of the alarm. Correct the specified problem and all correlated alarms should clear. See section 3.4 for a sample configuration problem. If alarms still exist, perform Procedure 3-5.

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 will not clear the alarm on the affected object that you are investigating. Perform Procedure 3-5 to review related object information.

Procedure 3-5 To determine root cause using related objects

1 From the Alarm Info form for the affected object (see Procedure 3-4), click on the Related Objects tab button. The Related Objects form opens, as shown in Figure 3-4.

Figure 3-4 Related Objects



```
network:10.1.200.52
network:10.1.200.52:router-1
network:10.1.200.52:router-1:ip-interface-3
network:10.1.200.53
network:10.1.200.53:lag
network:10.1.200.53:lag:interface-1
network:10.1.200.53:router-1
network:10.1.200.53:router-1:ip-interface-3
network:10.1.200.53:router-1:mpls
network:10.1.200.53:router-1:mpls:interface-3
```

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.

The Propagated tab button identifies objects higher in the managed object hierarchy that have problems resulting from the state of the affected object. 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 Choose this object in the Related Objects list and click on the View Object button. The object information form opens.

> **Note —** When you click on the Faults tab button, it should confirm that there are no alarms on this object. Alarms are listed in the dynamic alarm list.

4 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.

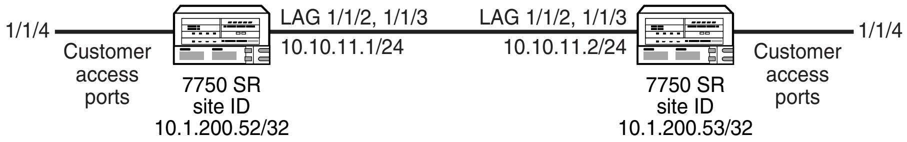
If necessary, check the Administrative State of the supporting port objects. A port with Administrative State Down does not generate alarms on the port, card, shelf, LAG, protocols, or sessions, but generates network path and service alarms. If the Administrative State is Down, change it to Up.

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

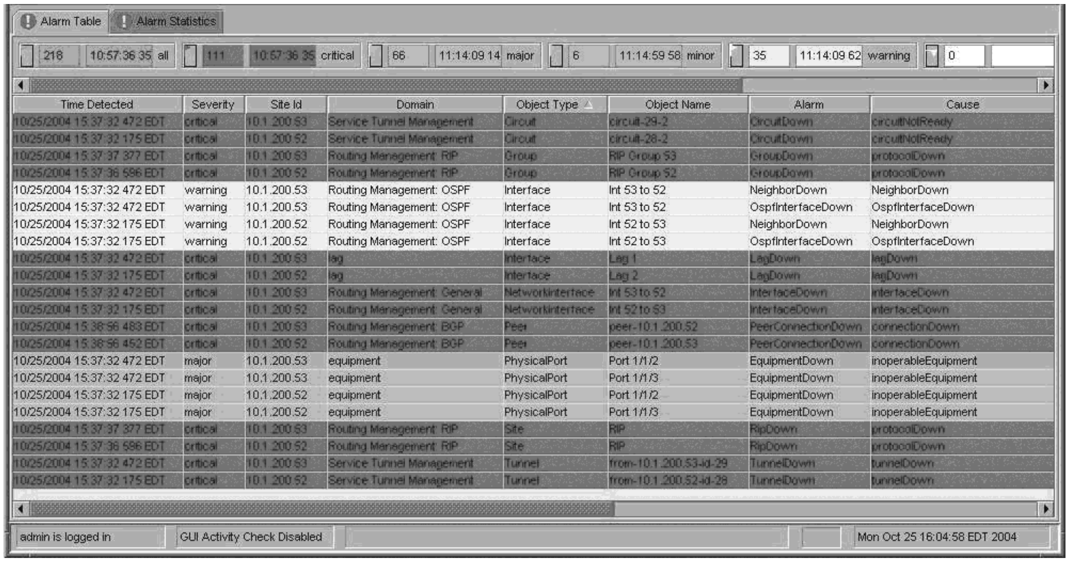
The dynamic alarm list is used to troubleshoot the following types of problems that are created.

- 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 service alarm list_1



Time Detected	Severity	Site Id	Domain	Object Type	Object Name	Alarm	Cause
10/25/2004 15:37:32 472 EDT	critical	10.1.200.53	Service Tunnel Management	Circuit	circuit-29-2	CircuitDown	circuitNotReady
10/25/2004 15:37:32 175 EDT	critical	10.1.200.52	Service Tunnel Management	Circuit	circuit-28-2	CircuitDown	circuitNotReady
10/25/2004 15:37:37 377 EDT	critical	10.1.200.53	Routing Management: RIP	Group	RIP Group 53	GroupDown	protocolDown
10/25/2004 15:37:36 596 EDT	critical	10.1.200.52	Routing Management: RIP	Group	RIP Group 52	GroupDown	protocolDown
10/25/2004 15:37:32 472 EDT	warning	10.1.200.53	Routing Management: OSPF	Interface	Int 53 to 52	NeighborDown	NeighborDown
10/25/2004 15:37:32 472 EDT	warning	10.1.200.53	Routing Management: OSPF	Interface	Int 53 to 52	OspfInterfaceDown	OspfInterfaceDown
10/25/2004 15:37:32 175 EDT	warning	10.1.200.52	Routing Management: OSPF	Interface	Int 52 to 53	NeighborDown	NeighborDown
10/25/2004 15:37:32 175 EDT	warning	10.1.200.52	Routing Management: OSPF	Interface	Int 52 to 53	OspfInterfaceDown	OspfInterfaceDown
10/25/2004 15:37:32 472 EDT	critical	10.1.200.53	lag	Interface	Lag 1	LagDown	lagDown
10/25/2004 15:37:32 175 EDT	critical	10.1.200.52	lag	Interface	Lag 2	LagDown	lagDown
10/25/2004 15:37:32 472 EDT	critical	10.1.200.53	Routing Management: General	NetworkInterface	Int 53 to 52	InterfaceDown	interfaceDown
10/25/2004 15:37:32 175 EDT	critical	10.1.200.52	Routing Management: General	NetworkInterface	Int 52 to 53	InterfaceDown	interfaceDown
10/25/2004 15:38:56 483 EDT	critical	10.1.200.53	Routing Management: BGP	Peer	peer-10.1.200.52	PeerConnectionDown	connectionDown
10/25/2004 15:38:56 452 EDT	critical	10.1.200.52	Routing Management: BGP	Peer	peer-10.1.200.53	PeerConnectionDown	connectionDown
10/25/2004 15:37:32 472 EDT	major	10.1.200.53	equipment	PhysicalPort	Port 1/1/2	EquipmentDown	inoperableEquipment
10/25/2004 15:37:32 472 EDT	major	10.1.200.53	equipment	PhysicalPort	Port 1/1/3	EquipmentDown	inoperableEquipment
10/25/2004 15:37:32 175 EDT	major	10.1.200.52	equipment	PhysicalPort	Port 1/1/2	EquipmentDown	inoperableEquipment
10/25/2004 15:37:32 175 EDT	major	10.1.200.52	equipment	PhysicalPort	Port 1/1/3	EquipmentDown	inoperableEquipment
10/25/2004 15:37:37 377 EDT	critical	10.1.200.53	Routing Management: RIP	Site	RIP	RipDown	protocolDown
10/25/2004 15:37:36 596 EDT	critical	10.1.200.52	Routing Management: RIP	Site	RIP	RipDown	protocolDown
10/25/2004 15:37:32 472 EDT	critical	10.1.200.53	Service Tunnel Management	Tunnel	from-10.1.200.53-id-29	TunnelDown	tunnelDown
10/25/2004 15:37:32 175 EDT	critical	10.1.200.52	Service Tunnel Management	Tunnel	from-10.1.200.52-id-28	TunnelDown	tunnelDown

The following procedure describes how to troubleshoot the problem.

Procedure 3-6 To troubleshoot a VPLS equipment problem

1 Review the alarms in the order that they are generated. When the Time Detected column shows that the alarms listed are generated at approximately the same time, it is a good indication that these alarms are 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 Object Info tab button, then click on the View Affected Object button to view state and other information about the object in the alarm.

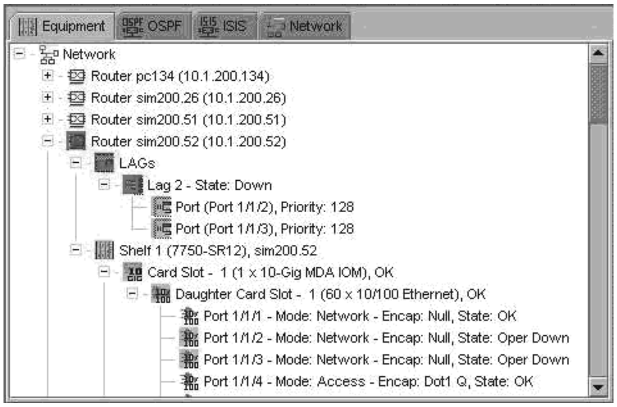
In this case, the Administrative State is Up and the Operational State is Down, which results in an alarm. The Operational state cannot be modified manually.

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 propagated alarms on objects up to the Router level as shown in Figure 3-7.

Figure 3-7 Equipment down and propagated alarms in navigation tree



```
Network
  Router pc134 (10.1.200.134)
  Router sim200.26 (10.1.200.26)
  Router sim200.51 (10.1.200.51)
  Router sim200.52 (10.1.200.52)
    LAGs
      Lag 2 - State: Down
        Port (Port 1/1/2), Priority: 128
        Port (Port 1/1/3), Priority: 128
    Shelf 1 (7750-SR12), sim200.52
      Card Slot -  1 (1 x 10-Gig MDA IOM), OK
        Daughter Card Slot -  1 (60 x 10/100 Ethernet), OK
          Port 1/1/1 - Mode: Network - Encap: Null, State: OK
          Port 1/1/2 - Mode: Network - Encap: Null, State: Oper Down
          Port 1/1/3 - Mode: Network - Encap: Null, State: Oper Down
          Port 1/1/4 - Mode: Access - Encap: Dot1 Q, State: OK
```

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

Procedure 3-7 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.

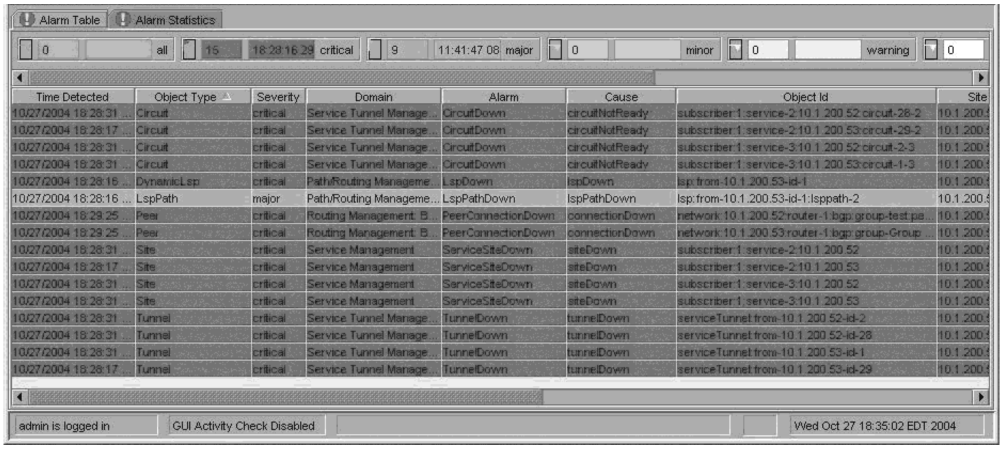
1 Check the physical connection to the port. The physical inspection shows that the two port connections supporting LAG 2 at Site 10.1.200.52. are not properly seated.

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 3-8.

Figure 3-8 VPLS service alarm list_2



0 all | 15 18:28:16 29 critical | 9 11:41:47 08 major | 0 minor | 0 warning | 0

Time Detected	Object Type	Severity	Domain	Alarm	Cause	Object Id	Site
10/27/2004 18:28:31 ...	Circuit	critical	Service Tunnel Manage...	CircuitDown	circuitNotReady	subscriber:1:service-2:10.1.200.52:circuit-28-2	10.1.200.
10/27/2004 18:28:17 ...	Circuit	critical	Service Tunnel Manage...	CircuitDown	circuitNotReady	subscriber:1:service-2:10.1.200.53:circuit-29-2	10.1.200.
10/27/2004 18:28:31 ...	Circuit	critical	Service Tunnel Manage...	CircuitDown	circuitNotReady	subscriber:1:service-3:10.1.200.52:circuit-2-3	10.1.200.
10/27/2004 18:28:31 ...	Circuit	critical	Service Tunnel Manage...	CircuitDown	circuitNotReady	subscriber:1:service-3:10.1.200.53:circuit-1-3	10.1.200.
10/27/2004 18:28:16 ...	DynamicLsp	critical	Path/Routing Manageme...	LspDown	lspDown	lsp:from-10.1.200.53-id-1	10.1.200.
10/27/2004 18:28:16 ...	LspPath	major	Path/Routing Manageme...	LspPathDown	lspPathDown	lsp:from-10.1.200.53-id-1:lsppath-2	10.1.200.
10/27/2004 18:29:25 ...	Peer	critical	Routing Management: B...	PeerConnectionDown	connectionDown	network:10.1.200.52:router-1:bgp:group-test:pe...	10.1.200.
10/27/2004 18:29:25 ...	Peer	critical	Routing Management: B...	PeerConnectionDown	connectionDown	network:10.1.200.53:router-1:bgp:group-Group ...	10.1.200.
10/27/2004 18:28:31 ...	Site	critical	Service Management	ServiceSiteDown	siteDown	subscriber:1:service-2:10.1.200.52	10.1.200.
10/27/2004 18:28:17 ...	Site	critical	Service Management	ServiceSiteDown	siteDown	subscriber:1:service-2:10.1.200.53	10.1.200.
10/27/2004 18:28:31 ...	Site	critical	Service Management	ServiceSiteDown	siteDown	subscriber:1:service-3:10.1.200.52	10.1.200.
10/27/2004 18:28:31 ...	Site	critical	Service Management	ServiceSiteDown	siteDown	subscriber:1:service-3:10.1.200.53	10.1.200.
10/27/2004 18:28:31 ...	Tunnel	critical	Service Tunnel Manage...	TunnelDown	tunnelDown	serviceTunnel:from-10.1.200.52-id-2	10.1.200.
10/27/2004 18:28:31 ...	Tunnel	critical	Service Tunnel Manage...	TunnelDown	tunnelDown	serviceTunnel:from-10.1.200.52-id-28	10.1.200.
10/27/2004 18:28:31 ...	Tunnel	critical	Service Tunnel Manage...	TunnelDown	tunnelDown	serviceTunnel:from-10.1.200.53-id-1	10.1.200.
10/27/2004 18:28:17 ...	Tunnel	critical	Service Tunnel Manage...	TunnelDown	tunnelDown	serviceTunnel:from-10.1.200.53-id-29	10.1.200.

admin is logged in | GUI Activity Check Disabled | Wed Oct 27 18:35:02 EDT 2004

The following procedure describes how to troubleshoot the problem.

Procedure 3-8 To troubleshoot an underlying port state problem

1 The Time Detected column shows that 16 alarms are generated at approximately the same time, which is a good indication that these alarms are 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 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.

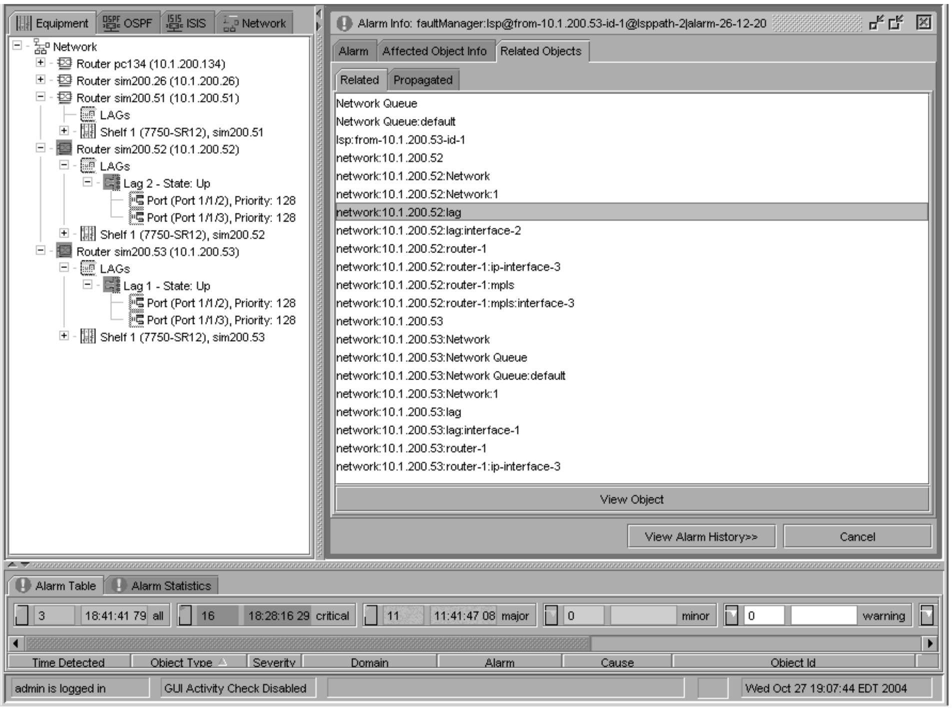
8 Click on the Affected Object Info tab button, then click on the View Affected Object button to view state and other information about the object in the alarm.

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

9 Check alarm description Table 3-14 for additional information, which in this case, indicates that the root cause may be a lower object in the managed object hierarchy.

10 Click on the Related Objects tab button on the Alarm Info form to display the managed objects related to the object in alarm, shown in Figure 3-9.

Figure 3-9 Lsp related objects in Alarm Info form



```
Network
  Router pc134 (10.1.200.134)
  Router sim200.26 (10.1.200.26)
  Router sim200.51 (10.1.200.51)
    LAGs
    Shelf 1 (7750-SR12), sim200.51
  Router sim200.52 (10.1.200.52)
    LAGs
      Lag 2 - State: Up
        Port (Port 1/1/2), Priority: 128
        Port (Port 1/1/3), Priority: 128
    Shelf 1 (7750-SR12), sim200.52
  Router sim200.53 (10.1.200.53)
    LAGs
      Lag 1 - State: Up
        Port (Port 1/1/2), Priority: 128
        Port (Port 1/1/3), Priority: 128
    Shelf 1 (7750-SR12), sim200.53
```

Alarm Info: faultManager:lsp@from-10.1.200.53-id-1@lsppath-2|alarm-26-12-20

```
Network Queue
Network Queue:default
lsp:from-10.1.200.53-id-1
network:10.1.200.52
network:10.1.200.52:Network
network:10.1.200.52:Network:1
network:10.1.200.52:lag
network:10.1.200.52:lag:interface-2
network:10.1.200.52:router-1
network:10.1.200.52:router-1:ip-interface-3
network:10.1.200.52:router-1:mpls
network:10.1.200.52:router-1:mpls:interface-3
network:10.1.200.53
network:10.1.200.53:Network
network:10.1.200.53:Network Queue
network:10.1.200.53:Network Queue:default
network:10.1.200.53:Network:1
network:10.1.200.53:lag
network:10.1.200.53:lag:interface-1
network:10.1.200.53:router-1
network:10.1.200.53:router-1:ip-interface-3
```

```
3  18:41:41 79 all   16  18:28:16 29 critical   11  11:41:47 08 major   0  minor   0  warning
```

```
admin is logged in   GUI Activity Check Disabled   Wed Oct 27 19:07:44 EDT 2004
```

11 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.

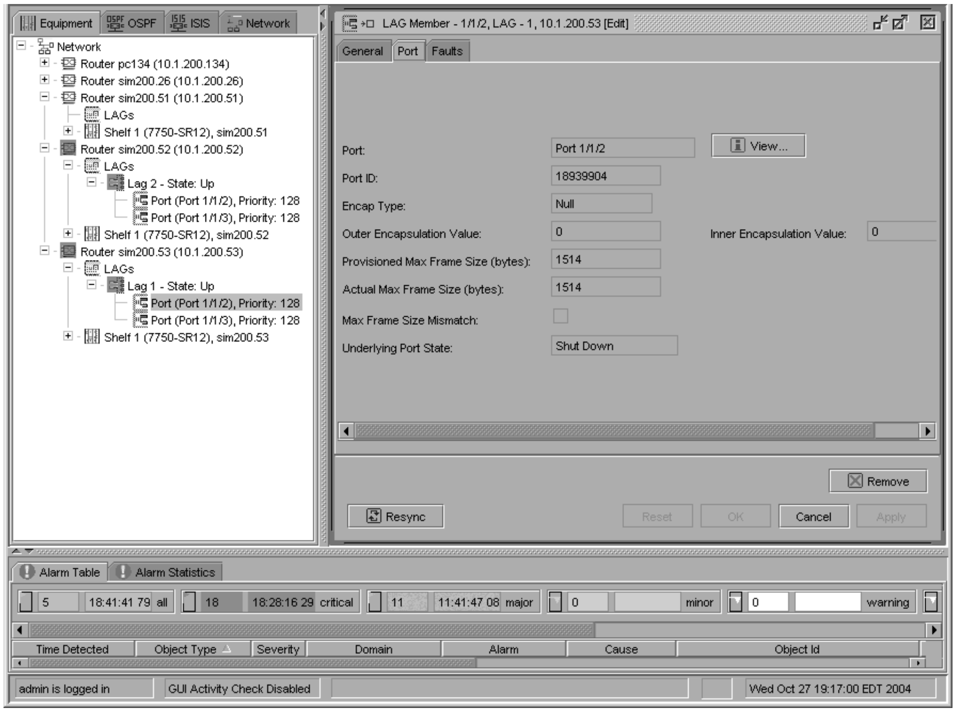
12 View the navigation tree Equipment tab button. It indicates that there are alarms related to both existing LAGs (Site Id 10.1.200.52 and Site Id 10.1.200.53). However, there is no LAG alarm in the dynamic alarm list and the LAG State is Up.

13 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 navigation tree Equipment view, 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 3-10. The LAG Member 1/1/2 properties form shows the Underlying Port State: Shut Down.

Figure 3-10 LAG member underlying port state in Properties form

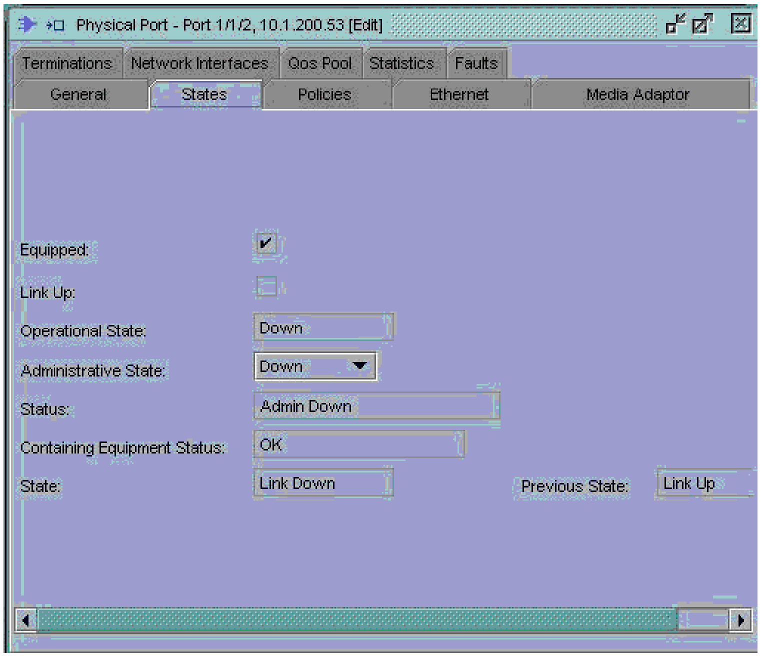

Equipment
OSPF
ISIS
Network
Network
Router pc134 (10.1.200.134)
Router sim200.26 (10.1.200.26)
Router sim200.51 (10.1.200.51)
LAGs
Shelf 1 (7750-SR12), sim200.51
Router sim200.52 (10.1.200.52)
LAGs
Lag 2 - State: Up
Port (Port 1/1/2), Priority: 128
Port (Port 1/1/3), Priority: 128
Shelf 1 (7750-SR12), sim200.52
Router sim200.53 (10.1.200.53)
LAGs
Lag 1 - State: Up
Port (Port 1/1/2), Priority: 128
Port (Port 1/1/3), Priority: 128
Shelf 1 (7750-SR12), sim200.53
LAG Member - 1/1/2, LAG - 1, 10.1.200.53 [Edit]
General
Port
Faults
View...
Remove
Resync
Reset
OK
Cancel
Apply
Alarm Table
Alarm Statistics
5
18:41:41 79
all
18
18:28:16 29
critical
11
11:41:47 08
major
0
minor
0
warning
Time Detected
Object Type
Severity
Domain
Alarm
Cause
Object Id
admin is logged in
GUI Activity Check Disabled
Wed Oct 27 19:17:00 EDT 2004

Port:	Port 1/1/2		
Port ID:	18939904		
Encap Type:	Null		
Outer Encapsulation Value:	0	Inner Encapsulation Value:	0
Provisioned Max Frame Size (bytes):	1514		
Actual Max Frame Size (bytes):	1514		
Max Frame Size Mismatch:	□		
Underlying Port State:	Shut Down		

iii Repeat step 13 ii for the second port. The LAG Member 1/1/3 properties form shows the State: Up.

14 In the navigation tree Equipment view, 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 3-11.

Figure 3-11 Physical port states in Properties form



Equipped:	☑
Link Up:	☐
Operational State:	Down
Administrative State:	Down
Status:	Admin Down
Containing Equipment Status:	OK
State:	Link Down
Previous State:	Link Up

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 3-9 to clear alarms related to an underlying port state problems.

Procedure 3-9 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 navigation tree Equipment view, 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 and choose Show Affected Object from the contextual menu. The affected object properties form opens.

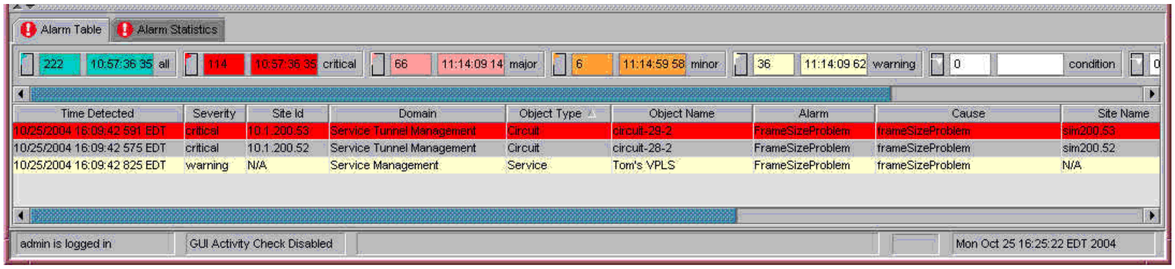
4 Click on the Resynch button. An Object deleted notification appears and the alarm clears automatically.

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 3-12.

Figure 3-12 VPLS service alarm list_3



Time Detected	Severity	Site Id	Domain	Object Type	Object Name	Alarm	Cause	Site Name
10/25/2004 16:09:42 591 EDT	critical	10.1.200.53	Service Tunnel Management	Circuit	circuit-29-2	FrameSizeProblem	frameSizeProblem	sim200.53
10/25/2004 16:09:42 575 EDT	critical	10.1.200.52	Service Tunnel Management	Circuit	circuit-28-2	FrameSizeProblem	frameSizeProblem	sim200.52
10/25/2004 16:09:42 825 EDT	warning	N/A	Service Management	Service	Tom's VPLS	FrameSizeProblem	frameSizeProblem	N/A

admin is logged in

GUI Activity Check Disabled

Mon Oct 25 16:25:22 EDT 2004

The following procedure describes how to troubleshoot the problem.

Procedure 3-10 To troubleshoot a VPLS configuration problem

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

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

3 Choose one of the two circuit alarms and acknowledge the alarm. In this example, the selected alarm is circuit alarm: Site ID 10.1.200.53.

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

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 circuit.
- Alarm type is configuration alarm.
- Probable cause is frame size problem.
- Domain is Service Tunnel Management.

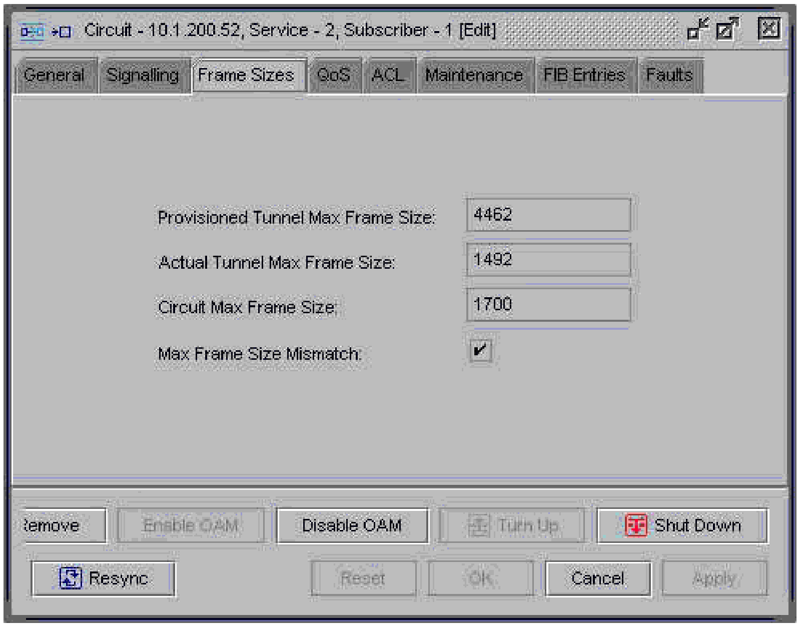
6 Click on the Affected Object Info tab button, then click on the View Affected Object button to determine the circuit states.

- 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 circuit object form to find more information about the problem, as shown in Figure 3-13.

Figure 3-13 Frame size configuration problem



Provisioned Tunnel Max Frame Size: 4462

Actual Tunnel Max Frame Size: 1492

Circuit Max Frame Size: 1700

Max Frame Size Mismatch: ☑

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

8 Check Table 3-24 for additional information about the Frame Size Problem alarm.

Perform procedure 3-11 to clear the Frame Size Problem alarm.

Procedure 3-11 To clear a Frame Size Problem (MTU Mismatch) alarm

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

1 Choose Service Management→Browse 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 Affected Object Id in the Alarm Info form for the alarm that you are trying to clear.

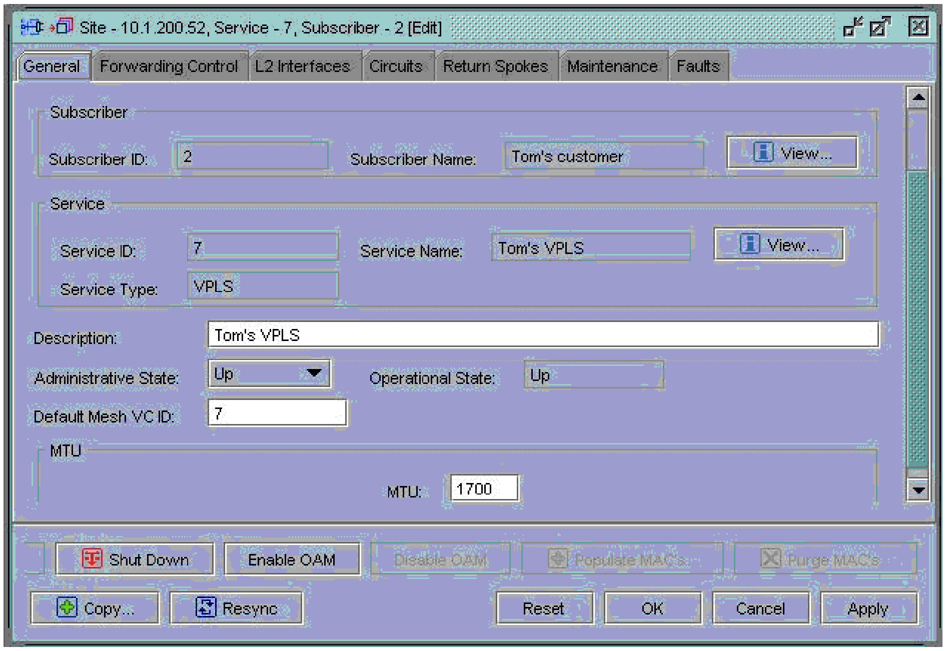
4 Click on the Edit button. The Service form opens.

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 Edit button. The Site form opens as shown in Figure 3-14.

Figure 3-14 Site form



Site - 10.1.200.52, Service - 7, Subscriber - 2 [Edit]

Subscriber

Subscriber ID: 2

Subscriber Name: Tom's customer

Service

Service ID: 7

Service Name: Tom's VPLS

Service Type: VPLS

Description: Tom's VPLS

Administrative State: Up

Operational State: Up

Default Mesh VC ID: 7

MTU

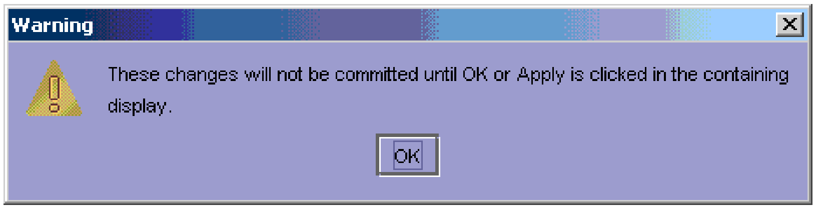
MTU: 1700

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

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 3-15. It warns you that changes to this Site form will not be applied to the service unless you click on the OK or Apply button in the Service form.

Figure 3-15 Warning to apply changes to all objects



These changes will not be committed until OK or Apply is clicked in the containing display.

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

11 Click the Apply button. The warning message, Figure 3-15, appears. It warns you that changes to this Service form will not be applied to the subscriber unless you click on the OK or Apply button in the Subscriber form

12 Click on the OK button. The Subscriber form appears.

13 Click on the Apply button. The MTU configuration change is applied to subscriber, service, and site objects. The circuit and related service alarms clear automatically.

3.5 Alarm description tables

Alarms are grouped by domain. Tables 3-2 to 3-31 describe the network object alarms that are raised on the 5620 SAM and are listed in domain alphabetical order.

Table 3-2 Bundle domain alarm

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Bundle Down ID: 152 Type: Equipment Alarm Probable cause: Bundle Down	Severity: critical Object type: Interface Domain: Bundle	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 3-3 DB domain alarm

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Database Backup Failed ID: 136 Type: Configuration Alarm Probable cause: Database Backup Failed	Severity: major Object type: Database Manager Domain: Db	The backup file could not be created because of, for example, lack of disk space or invalid write permissions.

Table 3-4 Equipment domain alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Data Loss ID: 148 Type: Equipment Alarm Probable cause: Data Loss	Severity: major Object type: Flash Memory Domain: equipment	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.
Name: Disk Capacity Problem ID: 144 Type: Equipment Alarm Probable cause: Disk Capacity Problem	Severity: *variable* Object type: Flash Memory Domain: equipment	The compact flash capacity threshold has been reached or exceeded on the router. These alarms start appearing when capacity reaches 75% or greater. This is a non-configurable threshold value. The severity of the alarm is *variable*, depending on the percentage of disk capacity used. When disk capacity equals: • 75% to 89%, severity is warning • 90% to 99%, severity is minor • 100% or greater, severity is major
Name: Equipment Down ID: 10 Type: Equipment Alarm Probable cause: Inoperable Equipment	Severity: major Object type: Equipment Domain: equipment	—
Name: Equipment Failure ID: 145 Type: Equipment Alarm Probable cause: Fan Failure	Severity: critical Object type: Fan Tray Domain: equipment	—
Name: Equipment In Test ID: 11 Type: Equipment Alarm Probable cause: Equipment In Test	Severity: warning Object type: Equipment Domain: equipment	—
Name: Equipment Mismatch ID: 9 Type: Equipment Alarm Probable cause: Equipment Type Mismatch	Severity: major Object type: Equipment Domain: equipment	—
Name: Equipment Removed ID: 8 Type: Equipment Alarm Probable cause: Replaceable Equipment Removed	Severity: major Object type: Equipment Domain: equipment	—
Name: Firmware Mismatch ID: 146 Type: Firmware Alarm Probable cause: Boot Rom Version Mismatch, FPGA Version Mismatch	Severity: critical Object type: Card Domain: equipment	A mismatch occurred between the firmware version and the software image on the router.

(1 of 2)

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Hardware Redundancy ID: 147 Type: Equipment Alarm Probable cause: Primary CPM Failure	Severity: major Object type: Control Processor Domain: equipment	—
Name: Link Down ID: 12 Type: Communications Alarm Probable cause: Port Link Problem	Severity: major Object type: Equipment Domain: equipment	—
Name: Software Failure ID: 149 Type: Software Alarm Probable cause: Load Failed	Severity: critical Object type: Replaceable Unit Domain: equipment	This alarm is generated when the CPM fails to load the software from the specified location.
Name: Temperature Threshold Crossed ID: 7 Type: Environmental Alarm Probable cause: Equipment Overheated	Severity: major Object type: Environment Domain: equipment	To display the temperature threshold, choose Equipment Manager->Cards tab->Environment.

(2 of 2)

Table 3-5 Generic alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Deployment Failure ID: 13 Type: Deployment Failure Probable cause: Failed To Modify Network Resource	Severity: minor Object type: Generic Object Domain: generic	Unable to create, modify, or delete a network object because there is intermittent or no IP connectivity to the network object, SNMP security parameters are incorrect, or SNMP is disabled on the router. Check the deployment tab using the 5620 SAM client GUI, as described in Procedure 8-4.
Name: Threshold Crossing Alarm ID: 14 Type: Threshold Crossed Probable cause: Threshold Crossed	Severity: warning Object type: Generic Object Domain: generic	—

Table 3-6 IGMP alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: CModeRxQuerMismatch ID: 172 Type: Protcol Alarm Probable cause: CModeRxQuerMismatch	Severity: warning Object type: IGMP Domain: igmp	—
Name: IGMP Down ID: 170 Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: IGMP Domain: igmp	
Name: QueryVerMismatch ID: 171 Type: Protocol Alarm Probable cause: QueryVerMismatch	Severity: warning Object type: IGMP Domain: igmp	

Table 3-7 L2 forwarding domain alarm

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Forwarding Table Size Limit Reached ID: 164 Type: Resource Alarm Probable cause: Resource Limit Reached	Severity: warning Object type: Site Fib Domain: l2fwd	Layer 2 FIB resource problem. Entries in the FIB are derived from the reachability information in the routing information base.

Table 3-8 L3 forwarding domain alarm

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Max Number of Multicast Routes ID: Type: Configuration Alarm Probable cause:	Severity: major Object type: Service Site Domain: l3fwd	—
Name: Multicast Routes Mid Level Threshold Reached ID: Type: Configuration Alarm Probable cause:	Severity: major Object type: Service Site Domain: l3fwd	—
Name: Route Distinguisher Not Configured ID: 142 Type: Configuration Alarm Probable cause: Route Distinguisher Not Configured	Severity: major Object type: Service Site Domain: l3fwd	There is a configuration problem on Layer 3 forwarding service site.

Table 3-9 layer 2 alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: IGMP Snooping Down ID: 174 Type: Protocol Alarm Probable cause: Protocol Down	Severity: warning Object type: layer 2 Domain: bridge	—
Name: MVR Site Down ID: 175 Type: Protocol Alarm Probable cause: Protocol Down	Severity: warning Object type: layer 2 Domain: TLS site	—
Name: TLS Site Down ID: 163 Type: Protocol Alarm Probable cause: Protocol Down	Severity: warning Object type: layer 2 Domain: TLS site	—

Table 3-10 LAG domain alarm

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Lag Down ID: 20 Type: Equipment Alarm Probable cause: Lag Down	Severity: critical Object type: Interface Domain: lag	All the ports in the LAG are operationally down.

Table 3-11 LDP domain alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Ldp Down ID: 22 Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Site Domain: ldp	—
Name: Ldp Interface Down ID: 21 Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Interface Domain: ldp	—
Name: Ldp Targeted Peer Down ID: 23 Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Targeted Peer Domain: ldp	This is an LDP configuration component.

Table 3-12 Mediation domain alarm

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Corrupt Image File ID: 158 Type: Configuration Alarm Probable cause: Invalid or Corrupt Image File	Severity: critical Object type: Software Folder Descriptor Domain: mediation	The image file indicated in the Software Upgrade Policy in SAMphone is corrupt.
Name: Ping Policy Misconfigured ID: 137 Type: Configuration Alarm Probable cause: Ping Command Execution Failed	Severity: warning Object type: Management Ping Policy Domain: mediation	—
Name: Software Image Root Path Misconfigured ID: 24 Type: Configuration Alarm Probable cause: File Path Problem	Severity: warning Object type: Software Upgrade Policy Domain: mediation	See the file path configured in the Software Upgrade Policy on the 5620 SAM.

Table 3-13 Network (netw) alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Activity Switch ID: 182 Type: Communication Alarm Probable cause: System Failed	Severity: Critical Object type: Nms System Domain: netw	—
Name: Boot Parameters Misconfigured ID: 35 Type: Configuration Alarm Probable cause: Persistent Index Failure	Severity: critical Object type: Network Element Domain: netw	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.
Name: Frame Size Problem ID: 37 Type: Configuration Alarm Probable cause: Management Connection Down	Severity: critical Object type: Statefull Connectable Interface Domain: netw	The MTU (sdp-mtu in CLI) defines the largest service frame size (in octets) that can be transmitted through an SDP to the far-end router, without requiring the packet to be fragmented. For other frame size alarms, see Tables 3-23 and 3-24.
Name: Inband Management Connection Down ID: 139 Type: Communication Alarm Probable cause: Management Connection Down	Severity: critical Object type: Node Discovery Control Domain: netw	—

(1 of 4)

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Interface Down ID: 36 Type: Interface Alarm Probable cause: Interface Down	Severity: critical Object type: Statefull Connectable Interface Domain: netw	—
Name: Management Interface Protection Switch ID: 34 Type: Communications Alarm Probable cause: Switch To Secondary	Severity: warning Object type: Network Element Domain: netw	—
Name: Module Out of Memory ID: 180 Type: Communications Alarm Probable cause: Out of Memory	Severity: critical Object type: Network Element Domain: netw	—
Name: Node Cold Start ID: 172 Type: Equipment Alarm Probable cause: Node Cold Start	Severity: warning Object type: Network Element Domain: netw	—
Name: Node Rebooted ID: 32 Type: Equipment Alarm Probable cause: Node Reboot	Severity: warning Object type: Network Element Domain: netw	—
Name: Node Upgraded ID: 178 Type: Configuration Alarm Probable cause: Upgraded Node Version	Severity: info Object type: Network Element Domain: netw	—
Name: Node Version Mismatch ID: 177 Type: Configuration Alarm Probable cause: Downgraded Node Version	Severity: critical Object type: Network Element Domain: netw	—
Name: Out of Band Management Connection Down ID: 138 Type: Communication Alarm Probable cause: Management Connection Down	Severity: critical Object type: Node Discovery Control Domain: netw	—
Name: Persistent Index Parameter Misconfigured ID: 173 Type: Configuration Alarm Probable cause: Persistent Index Configuration Mismatch	Severity: major Object type: Network Element Domain: netw	—

(2 of 4)

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Poller Problem ID: 31 Type: Communications Alarm Probable cause: Resync Failed	Severity: warning Object type: Network Element Domain: netw	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 devcies, and NIC card issues
Name: Redundancy Switchover ID: 181 Type: Equipment Alarm Probable cause: Redundancy Switchover	Severity: warning Object type: Network Element Domain: netw	—
Name: SNMP Authentication Failure ID: 176 Type: Authentication Alarm Probable cause: Auth Failure	Severity: warning Object type: Network Element Domain: netw	—
Name: SNMP Daemon Problem ID: 161 Type: Communication Alarm Probable cause: SNMP Daemon Error	Severity: warning Object type: Network Element Domain: netw	—
Name: SNMP Trap Dropped ID: 179 Type: Communication Alarm Probable cause: SNMP Daemon Overloaded	Severity: warning Object type: Network Element Domain: netw	—
Name: Standby CPM Management Connection Down ID: 140 Type: Communications Alarm Probable cause: Management Connection Down	Severity: critical Object type: Node Discovery Control Domain: netw	—
Name: Standby Host Status ID: 183 Type: Communication Alarm Probable cause: System Failed	Severity: Critical Object type: Nms System Domain: netw	—
Name: Trap Destination Misconfigured ID: 33 Type: Configuration Alarm Probable cause: Trap Destination Misconfigured	Severity: major Object type: Network Element Domain: netw	The SNMP trap destination configured on the router is not pointing to 5620 SAM.

(3 of 4)

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Trap Malformed ID: 135 Type: Communications Alarm Probable cause: Trap Schema Mismatch	Severity: major Object type: Network Element Domain: netw	—
Name: Upgraded Build Version Mismatch ID: 160 Type: Configuration Alarm Probable cause: Upgraded Image Not Booted	Severity: warning Object type: Network Element Domain: netw	—

(4 of 4)

Table 3-14 Path routing management: MPLS alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Lsp Down ID: 25 Type: Path Alarm Probable cause: Lsp Down	Severity: critical Object type: Lsp Domain: mpls	Verify the status of the underlying ports as a probable cause.
Name: Lsp Path Down ID: 26 Type: Path Alarm Probable cause: Lsp Path Down	Severity: major Object type: Lsp Path Domain: mpls	—
Name: Mpls Down ID: 27 Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Site Domain: mpls	—
Name: Path Reoptimized ID: 28 Type: Path Alarm Probable cause: Path Reoptimized	Severity: warning Object type: Tunnel Domain: mpls	—
Name: Path Rerouted ID: 29 Type: Path Alarm Probable cause: Path Rerouted	Severity: warning Object type: Tunnel Domain: mpls	—

Table 3-15 Policy domain alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Default Instance Inconsistency ID: 68 Type: Configuration Alarm Probable cause: Multiple Default Instances Encountered	Severity: warning Object type: Manager Domain: policy	—
Name: Template Inconsistency ID: 189 Type: Configuration Alarm Probable cause: Template Policy Mismatch	Severity: warning Object type: Manager Domain: policy	—

Table 3-16 Routing management: BGP domain alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Bgp Down ID: 6 Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Site Domain: bgp	—
Name: Peer Connection Down ID: 2 Type: Protocol Alarm Probable cause: connection Down (2)	Severity: critical Object type: Peer Domain: bgp	—
Name: Peer Down ID: 1 Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Peer Domain: bgp	—
Name: Peer Group Down ID: 5 Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Peer Group Domain: bgp	—
Name: Prefix Limit Exceeded ID: 4 Type: Protocol Alarm Probable cause: Prefix Limit Exceeded	Severity: major Object type: Peer Domain: bgp	The prefix-limit is the maximum number of routes BGP can learn from a peer.
Name: Prefix Limit Nearing ID: 3 Type: Protocol Alarm Probable cause: Prefix Limit Nearing	Severity: warning Object type: Peer Domain: bgp	—

Table 3-17 Routing management: ISIS domain alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Isis Adjacency Down ID: 153 Type: Protocol Alarm Probable cause: Protocol Down	Severity: minor Object type: Isis Adjacency Domain: isis	—
Name: Isis Area Mismatch ID: 156 Type: Configuration Alarm Probable cause: Area Type Misconfigured	Severity: warning Object type: Site Domain: isis	—
Name: Isis Auth Type Failure ID: 155 Type: Authentication Alarm Probable cause: Auth Failure	Severity: warning Object type: Site Domain: isis	—
Name: Isis Down ID: 19 Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Site Domain: isis	—
Name: Isis Manual Address Drops ID: 157 Type: Authentication Alarm Probable cause: No Error	Severity: warning Object type: Site Domain: isis	—
Name: Isis Rejected Adjacency ID: Type: Authentication Alarm Probable cause:	Severity: minor Object type: Site Domain: isis	—

Table 3-18 Routing management: OSPF domain alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Area Type Mismatch ID: 38 Type: Configuration Alarm Probable cause: Area Type Misconfigured	Severity: warning Object type: Area Domain: ospf	—
Name: Interface Db Descript Auth Failure ID: 46 Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Interface Domain: ospf	—
Name: Interface Db Descript Config ID: 40 Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Interface Domain: ospf	—

(1 of 4)

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Interface Hello Auth Failure ID: 45 Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Interface Domain: ospf	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 configured for the interface. The hello authentication type enables hello authentication at the interface or level context.
Name: Interface Hello Config ID: 39 Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Interface Domain: ospf	—
Name: Interface Ls Ack Auth Failure ID: 49 Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Interface Domain: ospf	—
Name: Interface Ls Ack Config ID: 43 Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Interface Domain: ospf	—
Name: Interface Ls Req Auth Failure ID: 47 Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Interface Domain: ospf	—
Name: Interface Ls Req Config ID: 41 Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Interface Domain: ospf	—
Name: Interface Ls Update Auth Failure ID: 48 Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Interface Domain: ospf	—
Name: Interface Ls Update Config ID: 42 Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Interface Domain: ospf	—
Name: Interface Null Packet Auth Failure ID: 50 Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Interface Domain: ospf	—
Name: Interface Null Packet Config ID: 44 Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Interface Domain: ospf	—

(2 of 4)

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Interface Rx Bad Packet ID: 51 Type: Communications Alarm Probable cause: Hello	Severity: warning Object type: Interface Domain: ospf	—
Name: Interface Tx Retransmit ID: 52 Type: Communications Alarm Probable cause: Hello	Severity: warning Object type: Interface Domain: ospf	The retransmit-interval for OSPF area interface determines how long (in seconds) OSPF waits before retransmitting an unacknowledged LSA to an OSPF neighbor.
Name: Lsdb Overflow ID: 53 Type: Equipment Alarm Probable cause: Resource Full	Severity: warning Object type: Site Domain: ospf	—
Name: Neighbor Down ID: 121 Type: Virtual Neighbor Down Probable cause: Virtual Neighbor Down	Severity: warning Object type: Virtual Link Domain: ospf	—
Name: Ospf Interface Down ID: 141 Type: Ospf Interface Down Probable cause: Ospf Interface Down	Severity: warning Object type: Interface Domain: ospf	—
Name: Virtual Link Down ID: 122 Type: Virtual Link Alarm Probable cause: Virtual Link Down	Severity: warning Object type: Virtual Link Domain: ospf	—
Name: Virtual Link Db Descript Auth Failure ID: 61 Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Virtual Link Domain: ospf	—
Name: Virtual Link Db Descript Config ID: 55 Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Virtual Link Domain: ospf	—
Name: Virtual Link Hello Auth Failure ID: 60 Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Virtual Link Domain: ospf	—
Name: Virtual Link Hello Config ID: 54 Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Virtual Link Domain: ospf	—
Name: Virtual Link Ls Ack Auth Failure ID: 64 Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Virtual Link Domain: ospf	—

(3 of 4)

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Virtual Link Ls Ack Config ID: 58 Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Virtual Link Domain: ospf	—
Name: Virtual Link Ls Req Auth Failure ID: 62 Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Virtual Link Domain: ospf	—
Name: Virtual Link Ls Req Config ID: 56 Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Virtual Link Domain: ospf	—
Name: Virtual Link Ls Update Auth Failure ID: 63 Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Virtual Link Domain: ospf	—
Name: Virtual Link Ls Update Config ID: 57 Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Virtual Link Domain: ospf	—
Name: Virtual Neighbor Down ID: 123 Type: Virtual Neighbor Down Probable cause: Virtual Neighbor Down	Severity: warning Object type: Virtual Link Domain: ospf	—
Name: Virtual Link Null Packet Auth Failure ID: 65 Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Virtual Link Domain: ospf	—
Name: Virtual Link Null Packet Config ID: 59 Type: Configuration Alarm Probable cause: Bad Version	Severity: warning Object type: Virtual Link Domain: ospf	—
Name: Virtual Link Rx Bad Packet ID: 66 Type: Communications Alarm Probable cause: Hello	Severity: warning Object type: Virtual Link Domain: ospf	—
Name: Virtual Link Tx Retransmit ID: 67 Type: Communications Alarm Probable cause: Hello	Severity: warning Object type: Virtual Link Domain: ospf	—

(4 of 4)

Table 3-19 Routing management: PIM domain alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Group in SSM Range ID: 187 Type: Configuration Alarm Probable cause: STARG Group in SSM Range	Severity: warning Object type: pim site Domain: PIM site	—
Name: Invalid Join Prune ID: 168 Type: Communcation Alarm Probable cause: Invalid Join Prune Received	Severity: warning Object type: pim site Domain: PIM site	—
Name: Invalid Register ID: 169 Type: Communication Alarm Probable cause: Invalid Join Register Received	Severity: warning Object type: PIM site Domain: PIM site	—
Name: Neighbor Loss ID: 188 Type: Communication Alarm Probable cause: Neighbor Connection Lost	Severity: warning Object type: Interface Domain: PIM site	—
Name: PIM Down ID: 184 Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: PIM site Domain: PIM site	—

Table 3-20 Routing management: RIP domain alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Group Down ID: 69 Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Group Domain: rip	—
Name: Rip Authentication Failure ID: 70 Type: Authentication Alarm Probable cause: Auth Failure	Severity: warning Object type: Interface Domain: rip	—

(1 of 2)

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Rip Authentication Mismatch ID: 71 Type: Authentication Alarm Probable cause: Auth Type Mismatch	Severity: warning Object type: Interface Domain: rip	—
Name: Rip Down ID: 72 Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Site Domain: rip	—

(2 of 2)

Table 3-21 Routing management: RSVP domain alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Rsvp Down ID: 74 Type: Protocol Alarm Probable cause: Protocol Down	Severity: critical Object type: Site Domain: rsvp	—
Name: Session Down ID: 73 Type: Protocol Alarm Probable cause: Interface Down	Severity: critical Object type: Session Domain: rsvp	—

Table 3-22 Security domain alarm

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Authentication Failure ID: 128 Type: Communications Alarm Probable cause: multiple Failed Login Attempts	Severity: warning Object type: TSecurity Manager Domain: security	At lease five attempts to log in to a 5620 SAM client have failed.
Name: Licensed CLE Limit Exceeded ID: 170 Type: Licensing Alarm Probable cause: Licensed Limit Exceeded	Severity: critical Object type: License Domain: security	Choose the Help->View Licence Info to display the Licence information on the 5620 SAM.
Name: Licensed CLE Limit Nearing ID: 168 Type: Licensing Alarm Probable cause: Licensed Limit Nearing	Severity: warning Object type: License Domain: security	

(1 of 2)

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Licensed Limit Exceeded ID: 127 Type: Communications Alarm Probable cause: Unsupported Sec Level	Severity: warning Object type: Mediation Policy Domain: security	—
Name: Licensed MDA Limit Exceeded ID: 167 Type: Licensing Alarm Probable cause: Licensed Limit Exceeded	Severity: critical Object type: License Domain: security	Choose the Help->View Licence Info to display the Licence information on the 5620 SAM.
Name: Licensed MDA Limit Nearing ID: 165 Type: Licensing Alarm Probable cause: Licensed Limit Nearing	Severity: warning Object type: License Domain: security	
Name: Licensed MDA Limit Nearly Exceeded ID: 166 Type: Licensing Alarm Probable cause: Licensed Limit Nearly Exceeded	Severity: major Object type: License Domain: security	

(2 of 2)

Table 3-23 Service management (svc) domain alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: MFib Table Size Limit Reached ID: 190 Type: Resource Alarm Probable cause: Resource Limit Reached	Severity: warning Object type: l2 Forwarding Domain: svc	—
Name: Mirror Destination Misconfigured ID: 197 Type: Configuration alarm Probable caus: Mirror Destination Misconfigured	Severity: major Object type: svc Domain: svc	—
Name: Service Site Down ID: 97 Type: Service Alarm Probable cause: Site Down	Severity: critical Object type: Site Domain: svc	All SAPs on the site are operationally down, or the service tunnels to the site are operationally down.
Name: Topology Misconfigured ID: 95 Type: Configuration Alarm Probable cause: Topology Misconfigured	Severity: critical Object type: Service Domain: svc	The service type for the same service ID is different on another router.
Name: Type Mismatch ID: 96 Type: Configuration Alarm Probable cause: Service Site Type Misconfigured	Severity: critical Object type: Service Domain: svc	—

Table 3-24 Service tunnel management (svt) domain alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Circuit Down ID: 99 Type: Circuit Alarm Probable cause: circuit Not Ready	Severity: critical Object type: Circuit Domain: svt	The underlying LSP is operationally down, or the LDP sessions are down.
Name: Keep Alive Problem ID: 100 Type: Oam Alarm Probable cause: keep Alive Failed	Severity: warning Object type: Tunnel Domain: svt	—
Name: Label Problem ID: 98 Type: Circuit Alarm Probable cause: label Problem	Severity: critical Object type: Circuit Domain: svt	—
Name: Tunnel Down ID: 30 Type: Path Alarm Probable cause: tunnel Down	Severity: critical Object type: Tunnel Domain: svt	A service tunnel (SDP) is down because the LSP that was relying on it is down.

Table 3-25 Site (sitesec) domain alarm

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Management Access Filter Misconfigured ID: 76 Type: Configuration Alarm Probable cause: Invalid Source Port Identifier	Severity: warning Object type: Maf Entry Domain: sitesec	Management access filters are used to restrict management of the 7750 SR 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 3-26 SNMP domain alarm

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Mediation Authentication Failure ID: 75 Type: Communications Alarm Probable cause: No Mediation Policy Found	Severity: critical Object type: Poller Manager Domain: snmp	—

Table 3-27 Software (sw) domain alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Boot Environment Sync Failed ID: 101 Type: Equipment Alarm Probable cause: boot Environment Sync Failed	Severity: critical Object type: Backup Restore Manager Domain: sw	Synchronization of bof file between CPM cards failed.
Name: Bootable Config Backup Failed ID: 103 Type: Configuration Alarm Probable cause: file Transfer Failure	Severity: major Object type: Backup Restore Manager Domain: sw	5620 SAM failed to back up the 7x50 node configuration files.
Name: Bootable Config Restore Failed ID: 104 Type: Configuration Alarm Probable cause: file Transfer Failure	Severity: major Object type: Backup Restore Manager Domain: sw	5620 SAM failed to backup the 7x50 node configuration files.
Name: Config File Sync Failed ID: 102 Type: Equipment Alarm Probable cause: config File Sync Failed	Severity: critical Object type: Backup Restore Manager Domain: sw	Synchronization of the configuration file between CPM cards failed.
Name: Hardware Boot Failure ID: 108 Type: Software Alarm Probable cause: software Boot Problem Due To Hardware Issues	Severity: critical Object type: Card Software Domain: sw	7x50 software failed to boot because of hardware issue(s).
Name: Primary Image Boot Failure ID: 191 Type: Configuration Alarm Probable cause: boot Option File Misconfigured	Severity: warning Object type: Card Software Domain: sw	—
Name: Save Config Failed ID: 105 Type: Configuration Alarm Probable cause: file Access Error	Severity: major Object type: Backup Restore Manager Domain: sw	The admin save command failed on the 7750 SR.
Name: Software Boot Failure ID: 107 Type: Software Alarm Probable cause: software Boot Problem	Severity: major Object type: Card Software Domain: sw	—
Name: Software Downloading ID: 109 Type: Software Alarm Probable cause: software Downloading	Severity: warning Object type: Card Software Domain: sw	—
Name: Software Initialized ID: 111 Type: Software Alarm Probable cause: software Initialized	Severity: warning Object type: Card Software Domain: sw	—

(1 of 2)

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Software Initializing ID: 110 Type: Software Alarm Probable cause: software Initializing	Severity: warning Object type: Card Software Domain: sw	—
Name: Software Upgrade Failed ID: 106 Type: Configuration Alarm Probable cause: file Access Error	Severity: major Object type: Backup Restore Manager Domain: sw	The software upgrade using the 5620 SAM failed.

(2 of 2)

Table 3-28 SONET equipment (sonetequipment) alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Ber Line Signal Degradation ID: 88 Type: Communications Alarm Probable cause: Ber Line Signal Degradation	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment	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.
Name: Ber Line Signal Failure ID: 89 Type: Communications Alarm Probable cause: Ber Line Signal Failure	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment	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.
Name: Line Alarm Indication Signal ID: 84 Type: Communications Alarm Probable cause: Line Alarm Indication Signal	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment	Reports line alarm indication signal LAIS errors. When configured, LAIS alarms are raised and cleared.
Name: Line Error Condition ID: 94 Type: Communications Alarm Probable cause: line Error Condition	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment	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.
Name: Line Remote Defect Indication ID: 85 Type: Communications Alarm Probable cause: line Remote Defect Indication	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment	Reports line remote defect indication errors. LRDIs are caused by remote LOF, LOC, LOS. When configured, LRDI alarms are raised and cleared.
Name: Loss Of Clock ID: 83 Type: Communications Alarm Probable cause: Loss Of Clock	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment	Reports a LOC which causes the operational state of the port to be shut down.

(1 of 3)

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Path Alarm Indication Signal ID: 77 Type: Communications Alarm Probable cause: Path Alarm Indication Signal	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment	—
Name: Path Loss Of Pointer ID: 78 Type: Communications Alarm Probable cause: Path Loss Of Pointer	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment	—
Name: Path Remote Defect Indicator ID: 79 Type: Communications Alarm Probable cause: Path Remote Defect Indicator	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment	—
Name: Path B3 Error ID: 80 Type: Communications Alarm Probable cause: Path Loss Of Pointer	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment	—
Name: Path Payload Mismatch ID: 81 Type: Communications Alarm Probable cause: Path Payload Mismatch	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment	—
Name: Path Remote B3 Error ID: 82 Type: Communications Alarm Probable cause: Path Remote Defect Indication	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment	—
Name: Rx Section Synchronization Error ID: 93 Type: Communications Alarm Probable cause: Rx Section Synchronization Error	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment	Reports section synchronization failure as reported by the S1 byte. When configured, SS1F alarms are raised and cleared.
Name: Section B1 Error ID: 87 Type: Communications Alarm Probable cause: Section B1 Error	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment	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.
Name: Section Loss Of Frame ID: 90 Type: Communications Alarm Probable cause: section Loss Of Frame	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment	Reports SLOF errors. When configured, SLOF alarms are raised and cleared.
Name: Section Loss Of Signal ID: 91 Type: Communications Alarm Probable cause: section Loss Of Signal	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment	Reports a SLOS error on the transmit side. When configured, SLOS alarms are raised and cleared.

(2 of 3)

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Section S1 Failure ID: 86 Type: Communications Alarm Probable cause: section S1 Failure	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment	See THE Rx Section Synchronization Error alarm in this table.
Name: Sonet Path Alarm Indication Signal ID: 129 Type: Communications Alarm Probable cause: Path Alarm Indication Signal	Severity: major Object type: Sonet Channel Domain: sonetequipment	Reports PAIS errors. When configured, PAIS alarms are raised and cleared.
Name: Sonet Path B3 Error ID: 132 Type: Communications Alarm Probable cause: Path B3 Error	Severity: major Object type: Sonet Channel Domain: sonetequipment	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.
Name: Sonet Path Loss Of Pointer ID: 130 Type: Communications Alarm Probable cause: Path Loss Of Pointer	Severity: major Object type: Sonet Channel Domain: sonetequipment	Reports PLOP (per tributary) errors. When configured, PLOP traps are raised but not cleared.
Name: Sonet Path Payload Mismatch ID: 133 Type: Communications Alarm Probable cause: path Payload Mismatch	Severity: major Object type: Sonet Channel Domain: sonetequipment	Reports a PPLM. As a result, the channel is operationally down. When configured, PPLM traps are raised but not cleared.
Name: Sonet Path Remote B3 Error ID: 134 Type: Communications Alarm Probable cause: path Remote B3 Error	Severity: major Object type: Sonet Channel Domain: sonetequipment	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
Name: Sonet Path Remote Defect Indication ID: 131 Type: Communications Alarm Probable cause: path Remote Defect Indication	Severity: major Object type: Sonet Channel Domain: sonetequipment	Reports path remote defect indication errors. When configured, PAIS alarms are raised and cleared.
Name: Sonet Path Unequipped Path Error ID: 143 Type: Communications Alarm Probable cause: path Unequipped Path Error	Severity: major Object type: Sonet Channel Monitor Specifics Domain: sonetequipment	—
Name: Tx Section Synchronization Error ID: 92 Type: Communications Alarm Probable cause: Tx Section Synchronization Error	Severity: major Object type: Sonet Port Specifics Domain: sonetequipment	Reports SS1F alarms as reported by the S1 byte. When configured, SS1F alarms are raised and cleared.

(3 of 3)

Table 3-29 TDM equipment (tdmequipment) domain alarms

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: DS1E1 Alarm Indication Signal ID: 112 Type: Communications Alarm Probable cause: alarm Indication Signal	Severity: major Object type: DS1E1 Channel Specifics Domain: tdmequipment	—
Name: DS1E1 Looped ID: 126 Type: Communications Alarm Probable cause: far End Loopback	Severity: major Object type: DS1E1 Channel Specifics Domain: tdmequipment	—
Name: DS1E1 Loss Of Frame ID: 113 Type: Communications Alarm Probable cause: Loss Of Frame	Severity: major Object type: DS1E1 Channel Specifics Domain: tdmequipment	—
Name: DS1E1 Loss Of Signal ID: 124 Type: Communications Alarm Probable cause: loss Of Signal	Severity: major Object type: DS1E1 Channel Specifics Domain: tdmequipment	—
Name: DS1E1 Out Of Frame ID: 125 Type: Communications Alarm Probable cause: out Of Frame	Severity: major Object type: DS1E1 Channel Specifics Domain: tdmequipment	—
Name: DS1E1 Resource Availability Indicator ID: 114 Type: Communications Alarm Probable cause: resource Availability Indicator	Severity: major Object type: DS1E1 Channel Specifics Domain: tdmequipment	—
Name: DS3E3 Alarm Indication Signal ID: 115 Type: Communications Alarm Probable cause: alarm Indication Signal	Severity: major Object type: DS3E3 Channel Specifics Domain: tdmequipment	—
Name: DS3E3 Looped ID: 120 Type: Communications Alarm Probable cause: far End Loopback	Severity: major Object type: DS3E3 Channel Specifics Domain: tdmequipment	—
Name: DS3E3 Loss Of Signal ID: 116 Type: Communications Alarm Probable cause: loss Of Signal	Severity: major Object type: DS3E3 Channel Specifics Domain: tdmequipment	—

(1 of 2)

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: DS3E3 Out Of Frame ID: 117 Type: Communications Alarm Probable cause: out Of Frame	Severity: major Object type: DS3E3 Channel Specifics Domain: tdmequipment	—
Name: DS3E3 Resource Availability ID: 119 Type: Communications Alarm Probable cause: resource Availability Indicator	Severity: major Object type: DS3E3 Channel Specifics Domain: tdmequipment	—

(2 of 2)

Table 3-30 template domain alarm

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Child Template invalid ID: 193 Type: Configuration Alarm Probable cause: Referenced Object Invalid	Severity: major Object type: template Domain: template	—
Name: Dependent Object Deleted ID: 192 Type: Configuration Alarm Probable cause: Referenced Object Gone	Severity: major Object type: template Domain: template	—
Name: Parent Template invalid ID: 194 Type: Configuration Alarm Probable cause: Referenced Object Invalid	Severity: major Object type: template Domain: template binding	—

Table 3-31 vs domain alarm

Alarm name, ID, type, and default probable cause	Default Severity, object type	Additional information
Name: Undefined Scheduler Reference ID: 118 Type: Configuration Alarm Probable cause: undefined Scheduler Reference	Severity: warning Object type: Service Type Definition Domain: vs	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.

OAM diagnostics for troubleshooting services

The 5620 SAM supports the following configurable in-band and out-of-band, packet-based OAM tools to troubleshoot network services:

- MTU Ping
- Tunnel Ping
- Circuit Ping
- LSP Ping
- LSP Trace
- MAC Ping
- MAC Trace
- MAC Populate
- MAC Purge
- VPRN Ping
- VPRN Trace

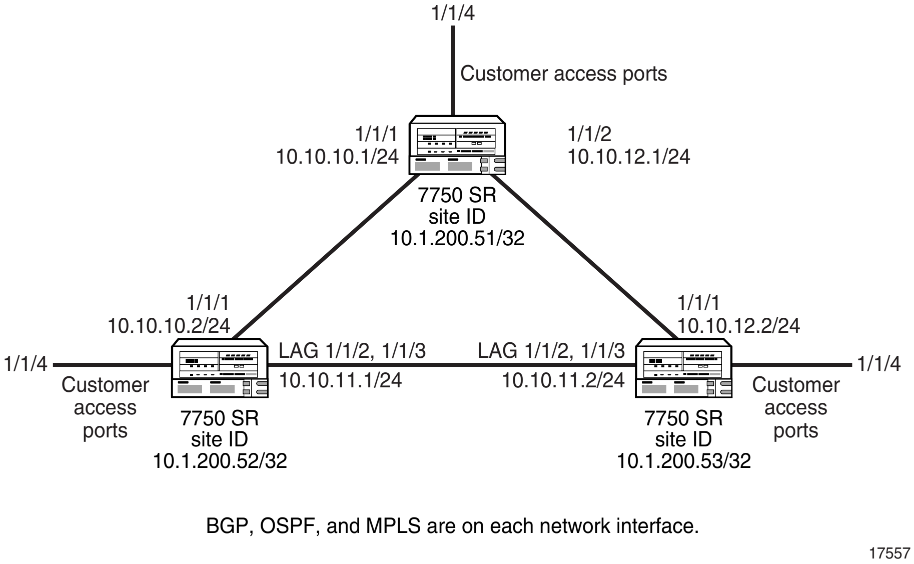
The procedures in this chapter use some of the OAM diagnostic tools in the workflow to troubleshoot a service. See the *5620 SAM User Guide* for descriptive information and how to enable and access the OAM diagnostics.

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

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 Browse 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.

You have completed the workflow for troubleshooting services. Contact your Alcatel technical support representative if the problem persists. See section 1.4 for more information.

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 Circuit 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.

You have completed the workflow for troubleshooting services. Contact your Alcatel technical support representative if the problem persists. See section 1.4 for more information.

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 Verify if the service problem still exists. If the service problem no longer exists, you have completed the workflow for troubleshooting service. If the service problem still exits, go to step 9.c.iv.

iv 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.

You have completed the workflow for troubleshooting services. Contact your Alcatel 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
Topology→Service Tunnel Manager	Search for and open a service tunnel, and use the OAM tools to ensure that the GRE or MPLS transport network topology is valid.
Service Management→Browse Services	Search for and open the service, site, or subscriber, and use the OAM tools to troubleshoot the service.
Topology→LSP Manager	Search for and open LSPs and LSP paths, and use the OAM tools to troubleshoot the MPLS LSP.

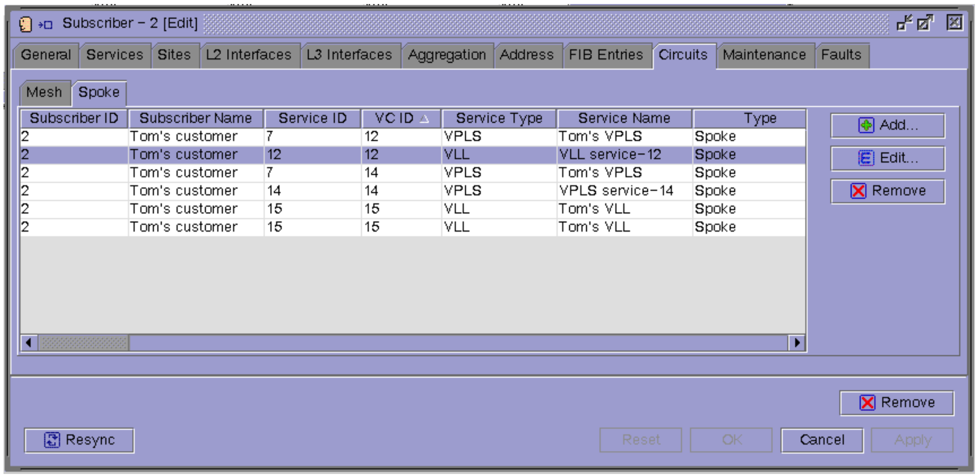
4.4 Service troubleshooting procedures

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 Service Management→Browse 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 associated with the service problem.
4. Click on the Edit button. The Service form opens.
5. Click on the Circuits 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. Figure 4-2 shows H-VPLS services sorted by VC IDs.

Figure 4-2 H-VPLS services sorted by VC IDs



Subscriber ID	Subscriber Name	Service ID	VC ID △	Service Type	Service Name	Type
2	Tom's customer	7	12	VPLS	Tom's VPLS	Spoke
2	Tom's customer	12	12	VLL	VLL service-12	Spoke
2	Tom's customer	7	14	VPLS	Tom's VPLS	Spoke
2	Tom's customer	14	14	VPLS	VPLS service-14	Spoke
2	Tom's customer	15	15	VLL	Tom's VLL	Spoke
2	Tom's customer	15	15	VLL	Tom's VLL	Spoke

If a VC ID has more than one unique Service ID, these services are involved in an H-VPLS relationship. For example, VC ID 12 has Service ID entries of 7 and 12.

a If there are no alarms on the H-VPLS service, go to step 5 in section 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 Sites tab button on the Services (Edit) form.

2 Review the states for the site using the Operational State and Administrative State columns.

3 Click on the L2 Interfaces, L3 Interfaces, and Circuits 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 section 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 5.

5 Implement and verify the solution for the service problem.

- If the problem no longer exists on the service, you have completed the troubleshooting workflow for services. Disable the OAM diagnostics to conserve system resources. See the *5620 SAM User Guide*.
- If the service problem persists, another type of problem may exist on your service. Go to section 4.2 and repeat the troubleshooting workflow. If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel 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 Interfaces tab button on the Services (Edit) form. A list of L2 interfaces appears.

2 Double-click on a row in the list. The L2 Interfaces 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 section 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.

iii Implement and verify the solution for the service problem.

- If the problem no longer exists on the service, you have completed the troubleshooting workflow for services. Disable the OAM diagnostics to conserve system resources. See the *5620 SAM User Guide*.
- If the service problem persists, another type of problem may exist on your service. Go to section 4.2 and repeat the troubleshooting workflow. If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel 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 Enable the OAM diagnostics for the service. See the *5620 SAM User Guide*.

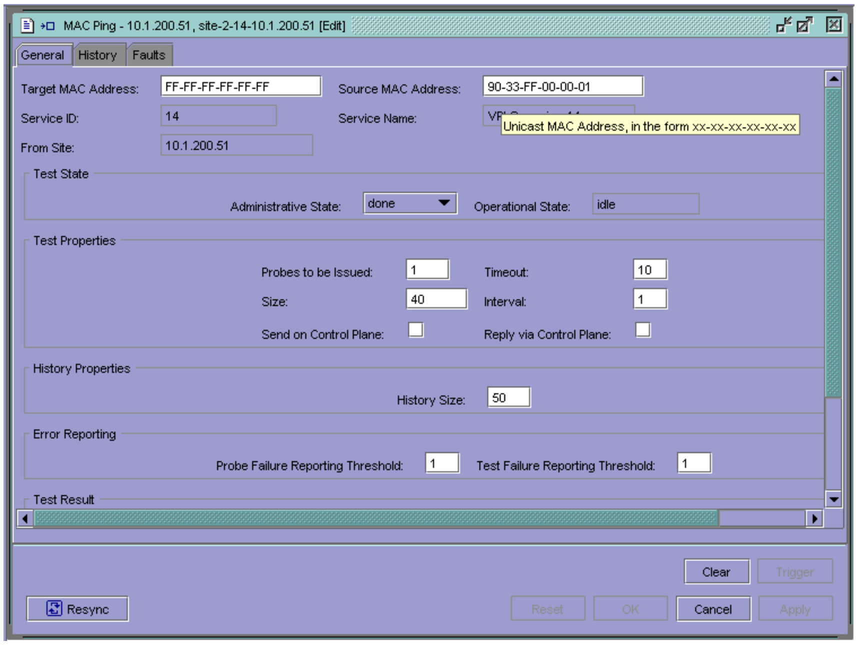
2 Open the MAC Ping configuration form and clear the results from the previous diagnostic session, if any.

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

3 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. Figure 4-3 shows the diagnostic configuration associated with a MAC Ping 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.

Figure 4-3 MAC Ping configuration form for a multiple address broadcast



MAC Ping - 10.1.200.51, site-2-14-10.1.200.51 [Edit]

Target MAC Address: FF-FF-FF-FF-FF-FF
Source MAC Address: 90-33-FF-00-00-01
Service ID: 14
Service Name: VP
Unicast MAC Address, in the form xx-xx-xx-xx-xx-xx
From Site: 10.1.200.51

Test State
Administrative State: done
Operational State: idle

Test Properties
Probes to be Issued: 1
Timeout: 10
Size: 40
Interval: 1
Send on Control Plane: □
Reply via Control Plane: □

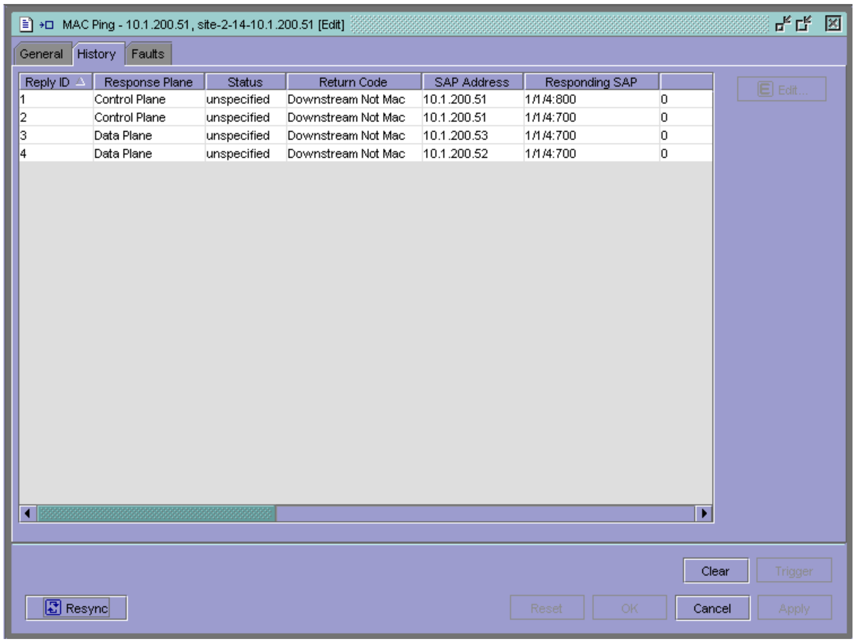
History Properties
History Size: 50

Error Reporting
Probe Failure Reporting Threshold: 1
Test Failure Reporting Threshold: 1

Test Result

Figure 4-4 shows the response associated with the diagnostic configuration in Figure 4-3.

Figure 4-4 MAC Ping results form for a multiple address broadcast

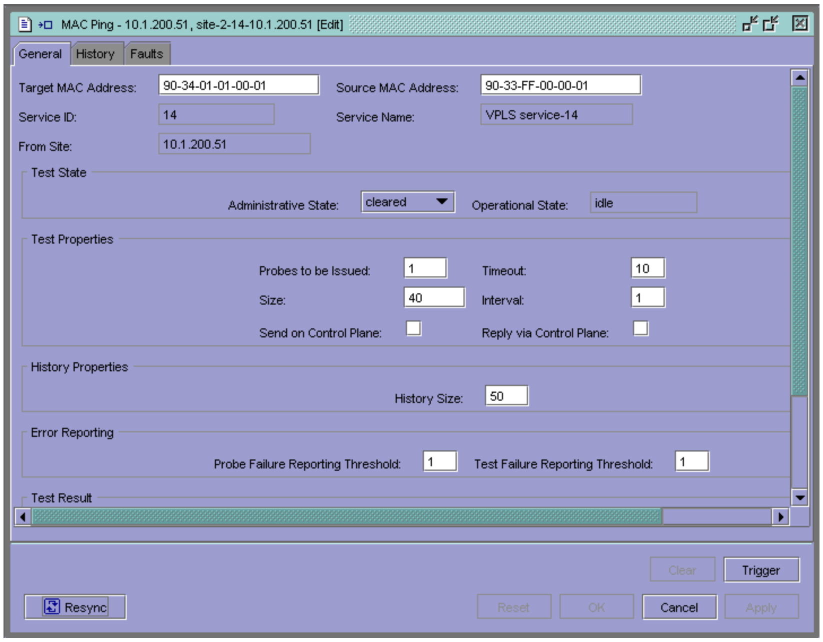


MAC Ping - 10.1.200.51, site-2-14-10.1.200.51 [Edit]

Reply ID	Response Plane	Status	Return Code	SAP Address	Responding SAP	
1	Control Plane	unspecified	Downstream Not Mac	10.1.200.51	1/1/4:800	0
2	Control Plane	unspecified	Downstream Not Mac	10.1.200.51	1/1/4:700	0
3	Data Plane	unspecified	Downstream Not Mac	10.1.200.53	1/1/4:700	0
4	Data Plane	unspecified	Downstream Not Mac	10.1.200.52	1/1/4:700	0

b Figure 4-5 shows the diagnostic configuration associated with a MAC Ping from site ID 10.1.200.51/32 to site ID 10.1.200.52/32 using the network in Figure 4-1.

Figure 4-5 MAC Ping configuration form for a node-to-node broadcast



MAC Ping - 10.1.200.51, site-2-14-10.1.200.51 [Edit]

Target MAC Address: 90-34-01-01-00-01
Source MAC Address: 90-33-FF-00-00-01
Service ID: 14
Service Name: VPLS service-14
From Site: 10.1.200.51

Test State
Administrative State: cleared
Operational State: idle

Test Properties
Probes to be Issued: 1
Timeout: 10
Size: 40
Interval: 1
Send on Control Plane: □
Reply via Control Plane: □

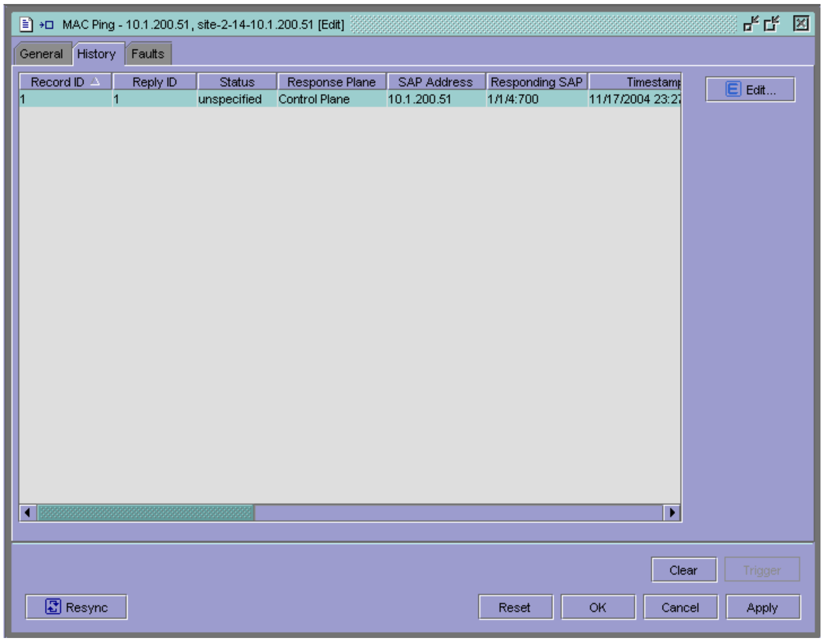
History Properties
History Size: 50

Error Reporting
Probe Failure Reporting Threshold: 1
Test Failure Reporting Threshold: 1

Test Result

Figure 4-6 shows the response associated with the diagnostic configuration in Figure 4-5.

Figure 4-6 MAC Ping results form for a node-to-node broadcast



Record ID	Reply ID	Status	Response Plane	SAP Address	Responding SAP	Timestamp
1	1	unspecified	Control Plane	10.1.200.51	1/1/4:700	11/17/2004 23:2

4 Review the diagnostic results and assess whether the configuration meets the network requirements. In particular, review the results in the Return Code column. Table 4-2 lists the displayed messages.

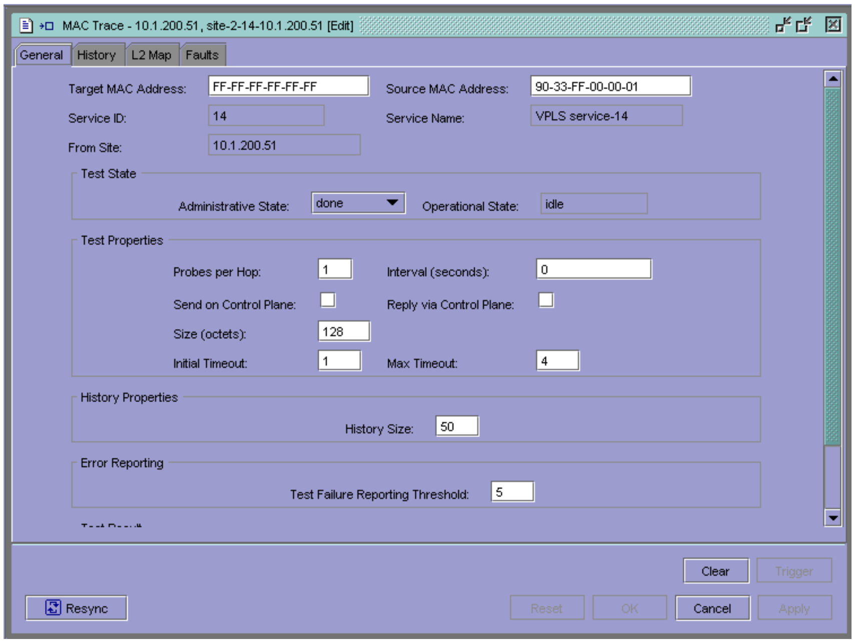
Table 4-2 MAC Ping OAM diagnostic results

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.

5 Open the MAC Trace configuration form and clear the results from the previous diagnostic session, if any.

6 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. Figure 4-7 shows the diagnostic configuration associated with a MAC Trace 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.

Figure 4-7 MAC Trace configuration form



MAC Trace - 10.1.200.51, site-2-14-10.1.200.51 [Edit]

Target MAC Address: FF-FF-FF-FF-FF-FF
Source MAC Address: 90-33-FF-00-00-01
Service ID: 14
Service Name: VPLS service-14
From Site: 10.1.200.51

Test State
Administrative State: done
Operational State: idle

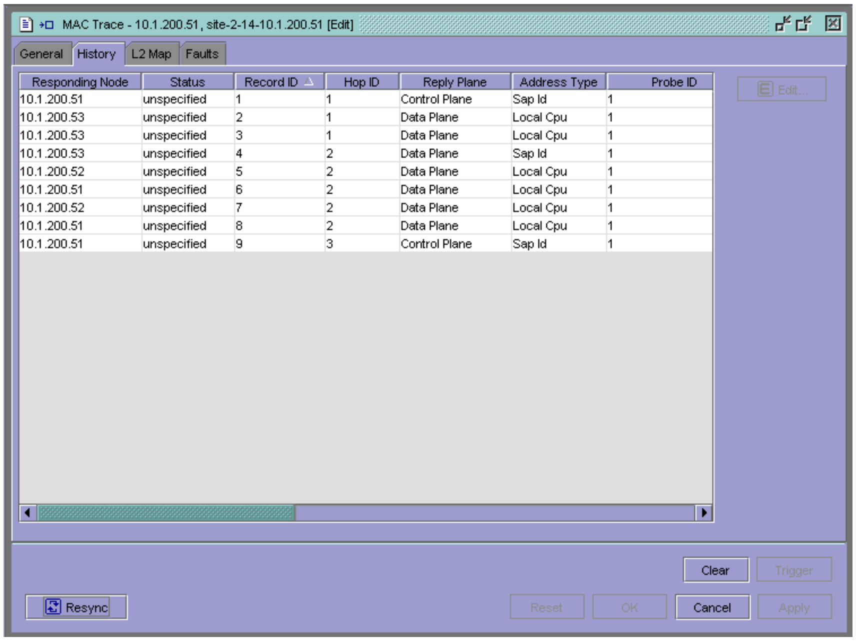
Test Properties
Probes per Hop: 1
Interval (seconds): 0
Send on Control Plane: □
Reply via Control Plane: □
Size (octets): 128
Initial Timeout: 1
Max Timeout: 4

History Properties
History Size: 50

Error Reporting
Test Failure Reporting Threshold: 5

Figure 4-8 shows the response associated with the diagnostic configuration in Figure 4-7.

Figure 4-8 MAC Trace results form



Responding Node	Status	Record ID	Hop ID	Reply Plane	Address Type	Probe ID
10.1.200.51	unspecified	1	1	Control Plane	Sap Id	1
10.1.200.53	unspecified	2	1	Data Plane	Local Cpu	1
10.1.200.53	unspecified	3	1	Data Plane	Local Cpu	1
10.1.200.53	unspecified	4	2	Data Plane	Sap Id	1
10.1.200.52	unspecified	5	2	Data Plane	Local Cpu	1
10.1.200.51	unspecified	6	2	Data Plane	Local Cpu	1
10.1.200.52	unspecified	7	2	Data Plane	Local Cpu	1
10.1.200.51	unspecified	8	2	Data Plane	Local Cpu	1
10.1.200.51	unspecified	9	3	Control Plane	Sap Id	1

7 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 section 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 section 4.2.

c Go to step 9.c in section 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 Enable the OAM diagnostics for the service. See the *5620 SAM User Guide*.

2 Record the maximum frame transmission size for the service.

3 Make sure that the OAM diagnostics are enabled on both circuits for the service tunnel.

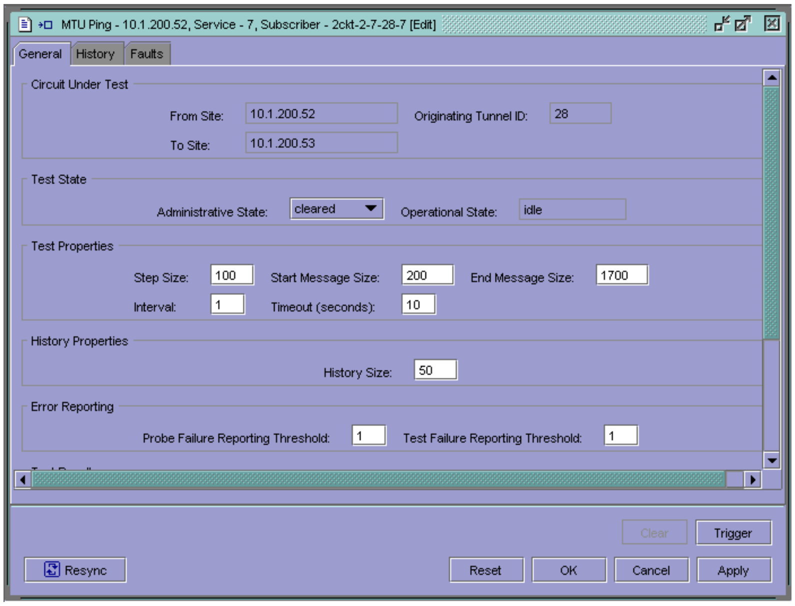
4 Open the MTU Ping configuration form and clear the results from the previous diagnostic session, if any.

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

5 Configure the parameters for the diagnostic session. Enter the MTU value recorded in step 2 in the End Message Size field.

6 Run the diagnostic. The MTU Ping increments the datagram size until it fails to pass through the SDP data path. Figure 4-9 shows the diagnostic configuration associated with a 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.

Figure 4-9 MTU Ping configuration form



MTU Ping - 10.1.200.52, Service - 7, Subscriber - 2ckt-2-7-28-7 [Edit]

Circuit Under Test

From Site: 10.1.200.52 Originating Tunnel ID: 28

To Site: 10.1.200.53

Test State

Administrative State: cleared Operational State: idle

Test Properties

Step Size: 100 Start Message Size: 200 End Message Size: 1700

Interval: 1 Timeout (seconds): 10

History Properties

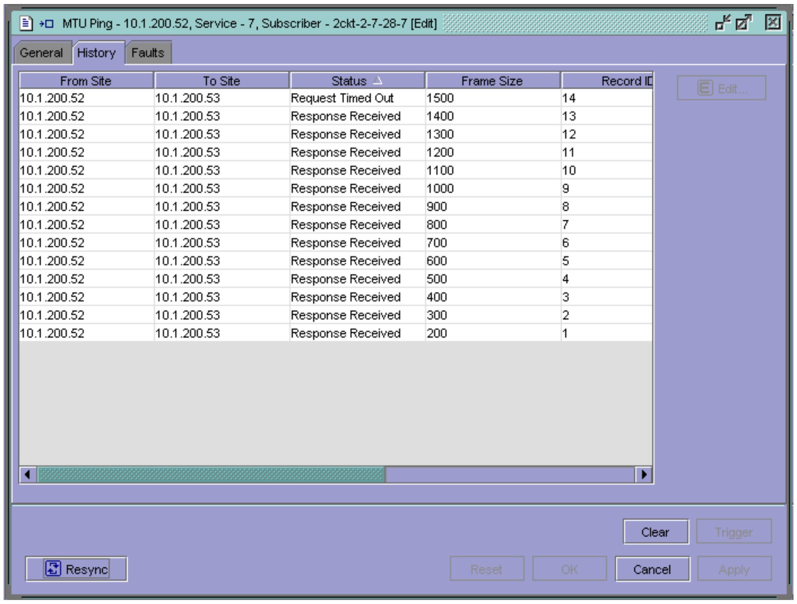
History Size: 50

Error Reporting

Probe Failure Reporting Threshold: 1 Test Failure Reporting Threshold: 1

Figure 4-10 shows the response associated with the diagnostic configuration in Figure 4-9.

Figure 4-10 MTU Ping results form



MTU Ping - 10.1.200.52, Service - 7, Subscriber - 2ckt-2-7-28-7 [Edit]

From Site	To Site	Status	Frame Size	Record ID
10.1.200.52	10.1.200.53	Request Timed Out	1500	14
10.1.200.52	10.1.200.53	Response Received	1400	13
10.1.200.52	10.1.200.53	Response Received	1300	12
10.1.200.52	10.1.200.53	Response Received	1200	11
10.1.200.52	10.1.200.53	Response Received	1100	10
10.1.200.52	10.1.200.53	Response Received	1000	9
10.1.200.52	10.1.200.53	Response Received	900	8
10.1.200.52	10.1.200.53	Response Received	800	7
10.1.200.52	10.1.200.53	Response Received	700	6
10.1.200.52	10.1.200.53	Response Received	600	5
10.1.200.52	10.1.200.53	Response Received	500	4
10.1.200.52	10.1.200.53	Response Received	400	3
10.1.200.52	10.1.200.53	Response Received	300	2
10.1.200.52	10.1.200.53	Response Received	200	1

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

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 section 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.

i Investigate the cause of the truncated packets.

ii Implement and verify the solution for the service problem.

- If the problem no longer exists on the service, you have completed the troubleshooting workflow for services. Disable the OAM diagnostics to conserve system resources. See the *5620 SAM User Guide*.
- If the service problem persists, another type of problem may exist on your service. Go to section 4.2 and repeat the troubleshooting workflow. If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel technical support representative. See section 1.4 for more information.

Procedure 4-6 To verify the end-to-end connectivity of a service using Circuit Ping

1 Enable the OAM diagnostics for the service. See the *5620 SAM User Guide*.

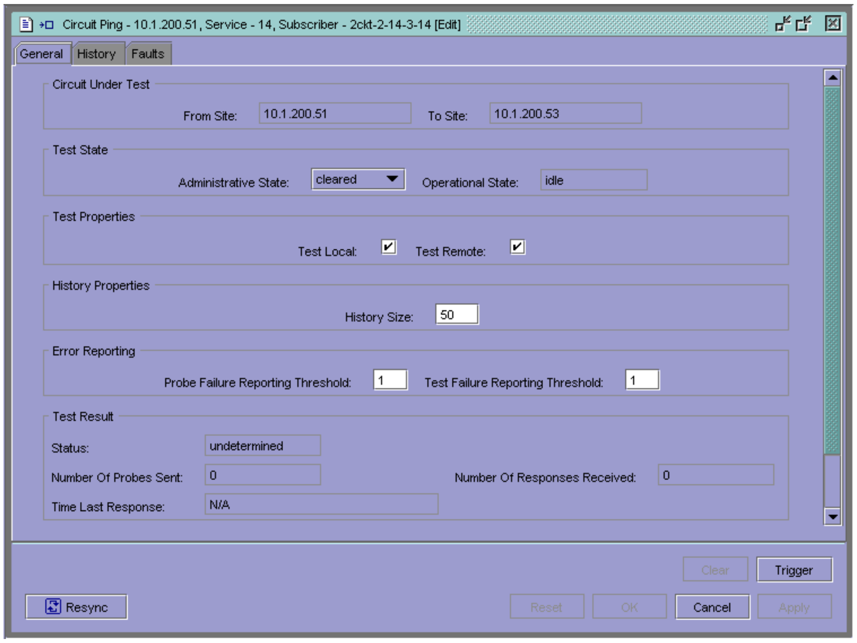
2 Open the Circuit Ping configuration form and clear the results from the previous diagnostic session, if any.

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

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

Figure 4-11 shows the diagnostic configuration associated with a Circuit Ping from site ID 10.1.200.51/32 to site ID 10.1.200.53/32 using the network in Figure 4-1.

Figure 4-11 Circuit Ping configuration form



Circuit Ping - 10.1.200.51, Service - 14, Subscriber - 2ckt-2-14-3-14 [Edit]

Circuit Under Test
From Site: 10.1.200.51
To Site: 10.1.200.53

Test State
Administrative State: cleared
Operational State: idle

Test Properties
Test Local: ☑
Test Remote: ☑

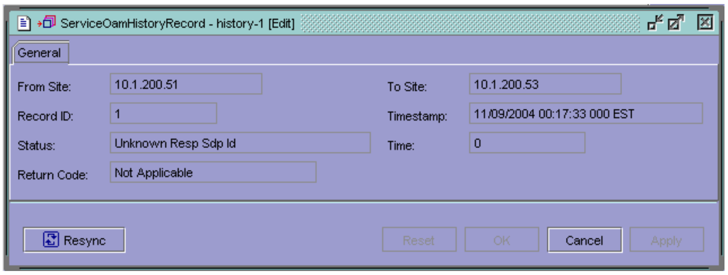
History Properties
History Size: 50

Error Reporting
Probe Failure Reporting Threshold: 1
Test Failure Reporting Threshold: 1

Test Result
Status: undetermined
Number Of Probes Sent: 0
Number Of Responses Received: 0
Time Last Response: N/A

Figure 4-12 shows the response associated with the diagnostic configuration in Figure 4-11. Double-click on the entry in the Circuit Ping results form to view the diagnostic details.

Figure 4-12 Circuit Ping results



ServiceOamHistoryRecord - history-1 [Edit]

From Site: 10.1.200.51
To Site: 10.1.200.53
Record ID: 1
Timestamp: 11/09/2004 00:17:33 000 EST
Status: Unknown Resp Sdp Id
Time: 0
Return Code: Not Applicable

4 Review the diagnostic results and assess whether the configuration meets the network requirements. Table 4-3 lists the displayed messages.

Table 4-3 Circuit 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 circuit 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

iii Implement and verify the solution for the service problem.

- If the problem no longer exists on the service, you have completed the troubleshooting workflow for services. Disable the OAM diagnostics to conserve system resources. See the *5620 SAM User Guide*.
- If the service problem persists, another type of problem may exist on your service. Go to section 4.2 and repeat the troubleshooting workflow. If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel technical support representative. See section 1.4 for more information.

b If the circuit 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 in section 4.2.

If the If the CLI IP ping fails, the two sites do not have IP connectivity. Go to step 5.

5 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.

iii Implement and verify the solution for the service problem.

- If the problem no longer exists on the service, you have completed the troubleshooting workflow for services. Disable the OAM diagnostics to conserve system resources. See the *5620 SAM User Guide*.
- If the service problem persists, another type of problem may exist on your service. Go to section 4.2 and repeat the troubleshooting workflow. If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel 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 Enable the OAM diagnostics for the service. See the *5620 SAM User Guide*.

2 Open the Tunnel Ping configuration form and clear the results from the previous diagnostic session, if any.

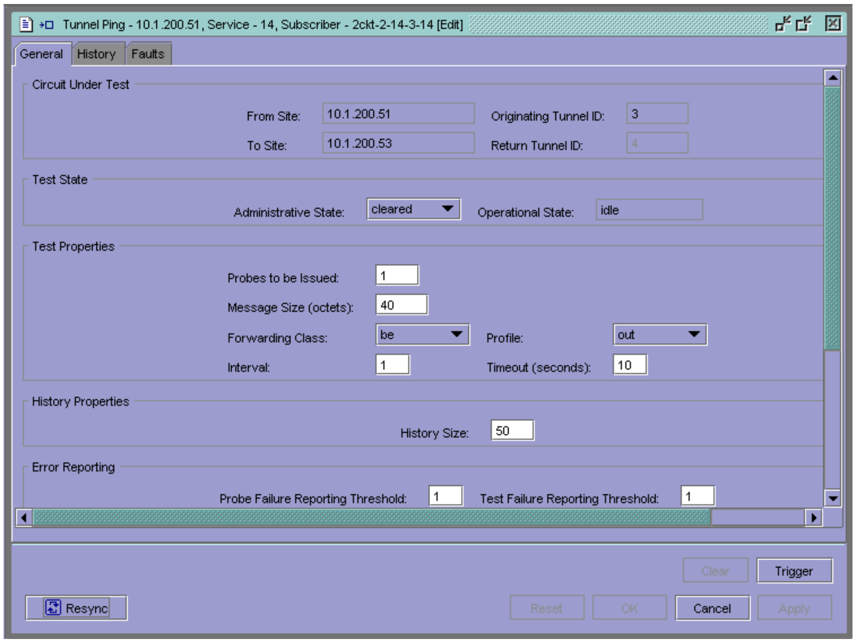
Note — You must use the Tunnel Ping diagnostic to test the service in both directions for the connection.

3 Configure the parameters for the diagnostic session as follows.

- Return Tunnel ID parameter must specify the return tunnel because the tunnels are unidirectional
- 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 subscriber services, such as VLL.
- Interval parameter must send multiple probes

4 Run the diagnostic. Figure 4-13 shows the diagnostic configuration associated with 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.

Figure 4-13 Tunnel Ping configuration form



Tunnel Ping - 10.1.200.51, Service - 14, Subscriber - 2ckt-2-14-3-14 [Edit]

Circuit Under Test

From Site: 10.1.200.51 Originating Tunnel ID: 3

To Site: 10.1.200.53 Return Tunnel ID: 4

Test State

Administrative State: cleared Operational State: idle

Test Properties

Probes to be Issued: 1

Message Size (octets): 40

Forwarding Class: be Profile: out

Interval: 1 Timeout (seconds): 10

History Properties

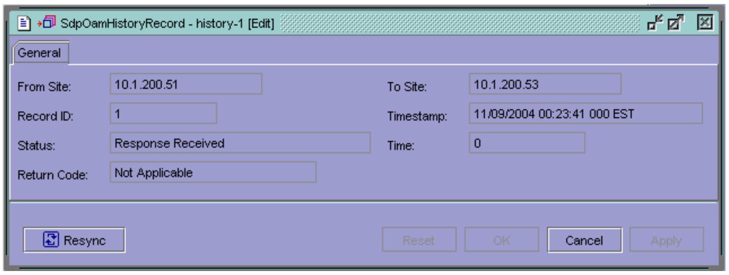
History Size: 50

Error Reporting

Probe Failure Reporting Threshold: 1 Test Failure Reporting Threshold: 1

Figure 4-14 shows the response associated with the diagnostic configuration in Figure 4-13. Double-click on the entry in the Tunnel Ping results form to view the diagnostic details.

Figure 4-14 Tunnel Ping results



SdpOamHistoryRecord - history-1 [Edit]

From Site: 10.1.200.51 To Site: 10.1.200.53

Record ID: 1 Timestamp: 11/09/2004 00:23:41 000 EST

Status: Response Received Time: 0

Return Code: Not Applicable

5 Review the diagnostic results and assess whether the configuration meets the network requirements. Table 4-4 lists the displayed messages.

Table 4-4 Tunnel OAM diagnostic results

Displayed message	Description
Request Timeout	The request timed out with a reply.
Orig-SDP Non-Existent	The request was not sent because the originating SDP does not exist.
Orig-SDP Admin-Down	The request was not sent because the originating SDP administrative state is Down.
Orig-SDP Oper-Down	The request was not sent because the originating SDP operational state is Down.

(1 of 2)

Displayed message	Description
Request Terminated	The operator terminated the request before a reply was received, or before the timeout of the request occurred.
Far End: Originator-ID Invalid	The request was received by the far-end, but the far-end indicates that the originating SDP ID is invalid.
Far End: Responder-ID Invalid	The request was received by the far-end, but the responder ID is not the same destination SDP ID that was specified.
Far End:Resp-SDP Non-Existent	The reply was received, but the return SDP ID used to respond to the request does not exist.
Far End:Resp-SDP Invalid	The reply was received, but the return SDP ID used to respond to the request is invalid.
Far End:Resp-SDP Down	The reply was received, but the return SDP ID indicates that the administrative or operational state of the SDP is Down.
Success	The tunnel is in service and working as expected. A reply was received without any errors.

(2 of 2)

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

You have completed the troubleshooting workflow for services.

- If the problem no longer exists on the service, you have completed the troubleshooting workflow for services. Disable the OAM diagnostics to conserve system resources. See the *5620 SAM User Guide*.
- If the service problem persists, another type of problem may exist on your service. Go to section 4.2 and repeat the troubleshooting workflow. If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel technical support representative. See section 1.4 for more information.

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

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

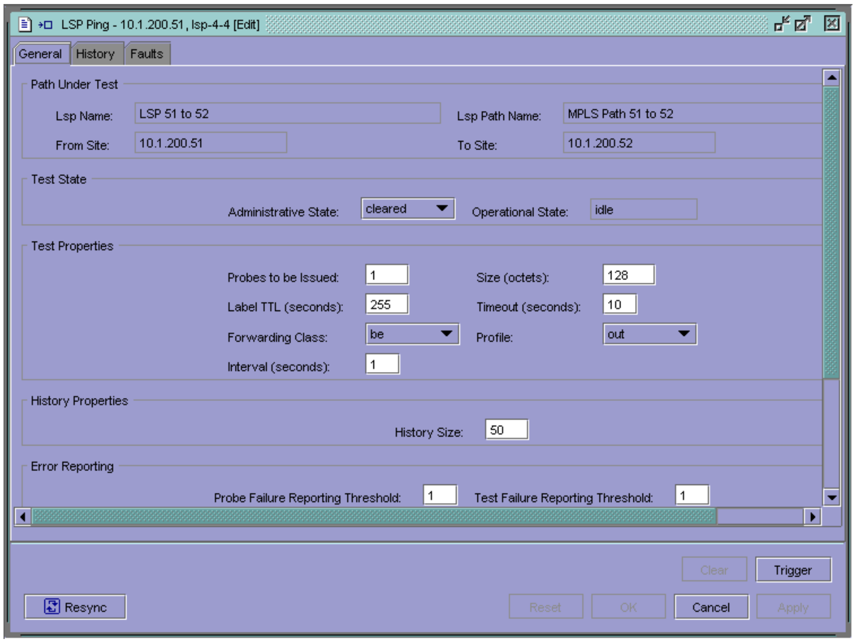
1 Enable the OAM diagnostics for the service. See the *5620 SAM User Guide*.

2 Open the LSP Ping configuration form and clear the results from the previous diagnostic session, if any.

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

3 Configure the parameters for the diagnostic session and run the diagnostic. Figure 4-15 shows the diagnostic configuration associated with 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.

Figure 4-15 LSP Ping configuration form



LSP Ping - 10.1.200.51, lsp-4-4 [Edit]

Path Under Test

Lsp Name: LSP 51 to 52
Lsp Path Name: MPLS Path 51 to 52
From Site: 10.1.200.51
To Site: 10.1.200.52

Test State

Administrative State: cleared
Operational State: idle

Test Properties

Probes to be Issued: 1
Size (octets): 128
Label TTL (seconds): 255
Timeout (seconds): 10
Forwarding Class: be
Profile: out
Interval (seconds): 1

History Properties

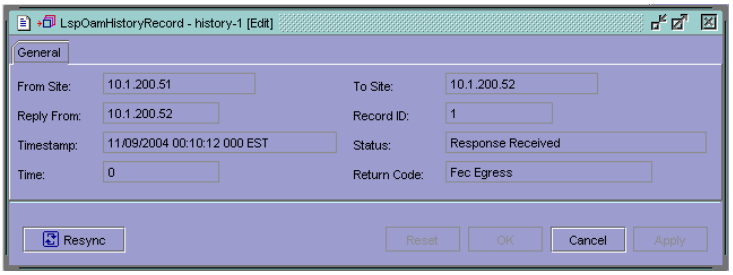
History Size: 50

Error Reporting

Probe Failure Reporting Threshold: 1
Test Failure Reporting Threshold: 1

Figure 4-16 shows the response associated with the diagnostic configuration in Figure 4-15. Double-click on the entry in the LSP Ping results form to view the diagnostic details.

Figure 4-16 LSP ping results



LspOamHistoryRecord - history-1 [Edit]

From Site: 10.1.200.51
To Site: 10.1.200.52
Reply From: 10.1.200.52
Record ID: 1
Timestamp: 11/09/2004 00:10:12 000 EST
Status: Response Received
Time: 0
Return Code: Fec Egress

4 Review the diagnostic results and assess whether the configuration meets the network requirements. Table 4-5 lists the displayed messages.

Table 4-5 LSP Ping OAM diagnostic results

Displayed message	Description
notApplicable (0)	The OAM diagnostic message does not apply to the OAM diagnostic performed.
fecEgress (1)	The replying router is an egress for the FEC. The far-end egress point exists and is operating correctly. No action required.
fecNoMap (2)	The replying router has no mapping for the FEC.
notDownstream (3)	The replying router is not a downstream router.

(1 of 2)

Displayed message	Description
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.

(2 of 2)

a If the LSP Ping passes, you have completed the workflow for troubleshooting services. Contact your Alcatel 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.

Implement and verify the solution for the service problem.

- If the problem no longer exists on the service, you have completed the troubleshooting workflow for services. Disable the OAM diagnostics to conserve system resources. See the *5620 SAM User Guide*.
- If the service problem persists, another type of problem may exist on your service. Go to section 4.2 and repeat the troubleshooting workflow. If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel technical support representative. See section 1.4 for more information.

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

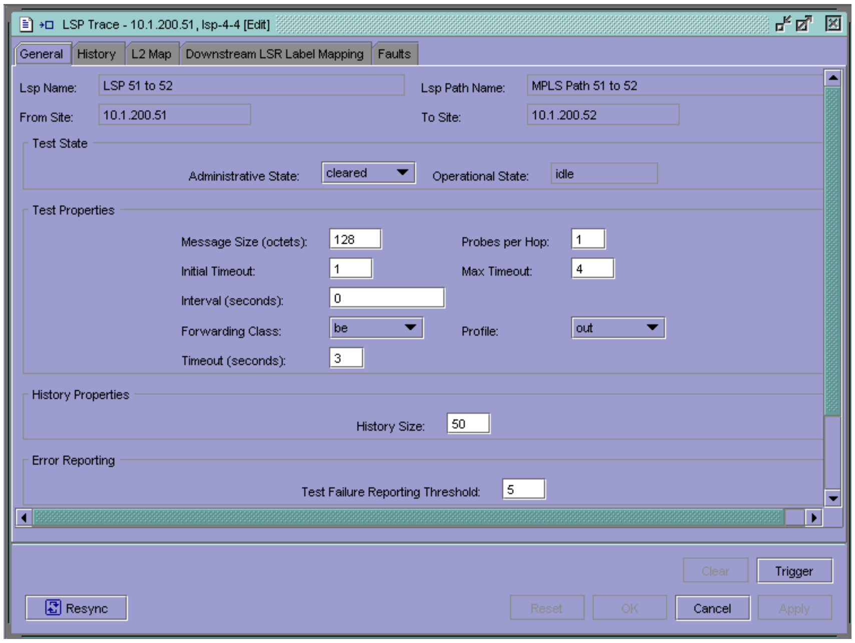
1 Enable the OAM diagnostics for the service. See the 5620 SAM User Guide.

2 Open the LSP Trace configuration form and clear the results from the previous diagnostic session, if any.

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

3 Configure the parameters for the diagnostic session and run the diagnostic. Figure 4-17 shows the diagnostic configuration associated with a LSP Trace from site ID 10.1.200.51/32 to site ID 10.1.200.52/32 using the network in Figure 4-1.

Figure 4-17 LSP Trace configuration form



LSP Trace - 10.1.200.51, lsp-4-4 [Edit]

Lsp Name: LSP 51 to 52

Lsp Path Name: MPLS Path 51 to 52

From Site: 10.1.200.51

To Site: 10.1.200.52

Test State

Administrative State: cleared

Operational State: idle

Test Properties

Message Size (octets): 128

Probes per Hop: 1

Initial Timeout: 1

Max Timeout: 4

Interval (seconds): 0

Forwarding Class: be

Profile: out

Timeout (seconds): 3

History Properties

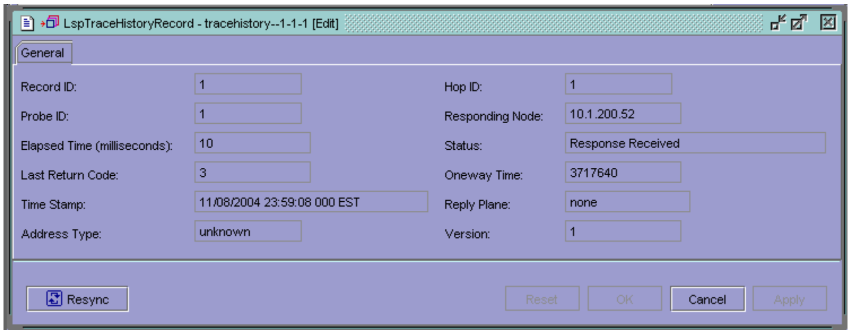
History Size: 50

Error Reporting

Test Failure Reporting Threshold: 5

Figure 4-18 shows the response associated with the diagnostic configuration in Figure 4-17. Double-click on the entry in the LSP Trace results form to view the diagnostic details.

Figure 4-18 LSP Trace results



LspTraceHistoryRecord - tracehistory--1-1-1 [Edit]

Record ID: 1

Hop ID: 1

Probe ID: 1

Responding Node: 10.1.200.52

Elapsed Time (milliseconds): 10

Status: Response Received

Last Return Code: 3

Oneway Time: 3717640

Time Stamp: 11/08/2004 23:59:08 000 EST

Reply Plane: none

Address Type: unknown

Version: 1

4 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, you have completed the workflow for troubleshooting services. Contact your Alcatel technical support representative if the problem persists. See section 1.4 for more information.

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.

Implement and verify the solution for the service problem.

- If the problem no longer exists on the service, you have completed the troubleshooting workflow for services. Disable the OAM diagnostics to conserve system resources. See the *5620 SAM User Guide*.
- If the service problem persists, another type of problem may exist on your service. Go to section 4.2 and repeat the troubleshooting workflow. If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel technical support representative. See section 1.4 for more information.

Procedure 4-10 To review the ACL filter

1 Click on the L2 Interfaces or L3 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 section 4.2.

b If there are ACL filtering configurations that interfere with the service traffic, implement and verify the solution for the service problem.

- If the problem no longer exists on the service, you have completed the troubleshooting workflow for services. Disable the OAM diagnostics to conserve system resources. See the *5620 SAM User Guide*.
- If the service problem persists, another type of problem may exist on your service. Go to section 4.2 and repeat the troubleshooting workflow. If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel technical support representative. See section 1.4 for more information.

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 subscriber 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
Tunnel view	Topology→Service Path Topology
LSP view	Topology→LSP Topology
MPLS provisioned path view	Topology→MPLS Path Manager Edit an MPLS path instance, click on the Provisioned Path tab button, and click on the Topology View button for the selected item.
MPLS cross connect view	Topology→LSP Manager Edit an LSP instance, click on the CrossConnect tab button, and click on the Topology View button for the selected item.
Subscriber view	Service Management→Manage Subscribers Select a subscriber 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
Large icon	Managed devices, such as a 7750 SR
Port icon	Managed access interface
Small icon	Unmanaged device, such as a PE router
Green lines	Provisioned paths for an LSP map. Network interface that is operationally up for all other maps.
Gray lines	Actual paths for an LSP map
Red lines	Network interface that is operationally down

Interpreting map status indicators

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

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

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

Table 5-3 Map status indicators

Indicator	Description
Icon color	The color of icons and links represent the operational status of the device. Red indicates that the device is operationally down. For a Subscriber view, red indicates that one or more of the services are operationally down. Yellow indicates that the device is being synchronized. Green indicates that the device is operationally up.
Upper left corner	Color and letter that indicate the most severe alarm on the device.
Upper right corner	Symbol that indicates connectivity to the device. This symbol corresponds to the icon color.

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
		Minor	Yellow
W	Blue	Warning	Cyan
—	—	Condition	Mocha
—	—	Cleared	Green
—	—	Info	Light blue
—	White	No alarm	—

Using map filters

You can restrict tunnel and LSP maps to network elements that match specified filter criteria, for example, to monitor specific status indicators or states.

Filters for the tunnel and LSP maps that may be useful for monitoring purposes include:

- Persistent Index Status
- Resync Status
- Config File Status

Filters can also be used to limit the number of devices and interfaces shown in a large or complex network, or to restrict the map to your area of responsibility.

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 If the map requires filters, choose the filter criteria.

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

4 You can use the Zoom In and Zoom Out buttons to adjust the map depending on the size of the network that you are viewing.

5 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

6 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 network element that has an alarm 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 Edit 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 networkstations 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 technical support representative. Table 6-1 lists the minimum bandwidth requirements in the network management domain.

Table 6-1 Minimum bandwidth requirements in the network management domain

Platform connection between a	Minimum bandwidth requirements
5620 SAM client and a 5620 SAM server	512 Kb/s for normal management connection 56 kb/s modem for basic troubleshooting and configurations
5620 SAM primary server and the 5620 SAM primary database to a standby server and database, co-located or distributed	1 Mb/s for servers 3 Mb/s for databases
5620 SAM server and one managed device using out-of-band management	From 200 to up to 650 kb/s for each managed device
5620 SAM server and single managed device	1 Mb/s
5620 SAM server and the maximum number of supported devices in a single management domain	10 Mb/s
5620 SAM server and an OSS application	1 Mb/s
5620 SAM active database to a standby database and an OSS application	10 Mb/s

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: Garbled text when connecting using a modem from a Solaris platform

When a call is placed, the dialing computer initiates the connection with the dialing modem by sending a dial command. The dialing modem never has a problem communicating with the dialing computer because it will autobaud to the right speed.

However, at the answering side, the modem initiates the connection with the answering computer. The serial port on the answering computer will not autobaud and may be configured for one specific speed, as set using admintool. The speed used by the modems depends on the configuration of the answering modem. Most modems are configured to set the speed of the serial port to something similar to the speed at which the connection to the remote modem operates. For example, if the modems negotiated a 26.6 kb/s baud connection, then it will set its serial port to 26.6 kb/s baud. If you set your port to 56 kb/s baud using admintool, you get garbled text.

The solution is to lock the serial port at a specific baud rate. The configuration command for doing this depends on the modem manufacturer. Look for “fixed DTE rate” in the modem documentation for the configuration command.

Procedure 6-3 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 6-4 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 6-4 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. Table 6-2 lists the default ports and their values.

Note — Track any changes to port configuration values for future reference.

Table 6-2 Firewall port default settings

Type	Default port number	Type	Description
5620 SAM server	1098 and 1099	TCP	org.jboss.naming.NavingService for client and 5620 SAM-O communication
	4444		org.jboss.invocation.jrmp.server.JRMPInvoker for client and 5620 SAM-O communication
	4445		org.jboss.invocation.pooled.server.PooledInvoker for client and 5620 SAM-O communication
	8080		HTTP 5620 SAM-O for client access
	8443		HTTPS 5620 SAM-O for client access
	8093		JMS for 5620 SAM-O
	162	UDP	SNMP traps
5620 SAM database	1521	TCP	JDBC
	9002		RMI database proxy port for switchover or failover requests
Managed devices	161	UDP	SNMP connections to the managed devices
	20 and 21	TCP	FTP (passive) connections to the managed devices
	22	TCP	SSH connections to the managed devices
	23	TCP	Telnet connections to the managed devices

Contact your technical support representative for more information about configuring ports that need to be open or protected by a firewall, depending on the system architecture.

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.

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.

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 Obtain the UNIX utility top and install the utility on the Solaris workstation.

2 Open a command or shell tool.

3 Change to the 5620 SAM install directory by typing:

cd /*install directory* ↵

where *install directory* is the installation directory of the 5620 SAM software

4 Run the top command to check for processes that are consuming CPU cycles:

i To list the top CPU processes using top, type:

top ↵

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. The displays are similar for top and prstat.

ii Review the output. The following is sample top output.

```
Last PID: 4099; load averages: 0.00, 0.01, 0.01

85 processes: 66 sleeping, 19 running, 1 on CPU

Cpu state: 0.0% idle, 99.8% user, 0.2% kernel, 0.0% oiwait,
0.0% swap

memory: 125M real, 4692K free, 151M swap, 176M free swap

PID  username  PRI  NICE  SIZE   RES   STATE

301    root     33   0     96M   77M   cpu

TIME   WCPU    CPU     COMMAND
```

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.

5 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

(1 of 2)

Heading	Description (events per second unless noted)
mjf	Major faults
xcal	Interprocessor cross-calls
intr	Interrupts
ithr	Interrupts as threads (not counting clock interrupts)
csw	Context switches When the csw number slowly increases and the platform is not I/O bound, a mutex contention is indicated
icsw	Involuntary context switches When the iscw number increases beyond 500, the system is considered to be under heavy load
migr	Thread migrations to another processor
smtx	Spins on mutexes (lock not acquired on first try) if the smtx number increases sharply, for instance from 30 to 300, a system resource bottleneck is indicated
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.

6 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:

- 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 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 descriptions

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 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 swapfilesizem 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 client GUI

8.1 Troubleshooting common client application problems

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

Procedure 8-1 Problem: Performance is slow across the clients

Possible causes are:

- 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 To check for LAN throughput issues:

i Open a command or shell tool.

ii To collect data to determine whether there is network bottleneck, type:

```
netstat -i s ↵
```

where *s* is the time, in seconds, over which you want to collect data. Alcatel recommends that you start with 50 s; this time interval may require adjusting to meet your specific requirements.

The -i parameter shows the state of the interfaces that are used for TCP/IP traffic.

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. There is another set of columns which display the results for all the interfaces. This sample only has one interface, so both sets of columns display the same result.

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 network bottlenecks.

iv To stop the netstat command, press CTRL-C.

2 Check that the client platform is appropriately sized. See the appropriate RLN for the software release that you are running.

Procedure 8-2 Problem: Unable to print from a 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
A user cannot delete a printer	There are print jobs in the queue for that printer	Delete the print jobs in the queue using the lprm command
The client cannot print	The printer was not added to the list of available printers	Add the printer to the list of printers by using the admintool

1 On the workstation, log in as the user experiencing printing problems.

2 Type the lp command that you want to use:

a To list jobs in the printer queue, type:

```
lpq ↵
```

When you run the lpq command and a message appears that the printer cannot be found, there is a connection problem between the PC or workstation and the printer. A printer cannot be found message may indicate that the environment variable for the printer is not set correctly, or that the machine is not configured to use the printer.

b To display information about the state of the printer, type:

```
lpstat ↵
```

When you run the lpstat command and a message appears that the printer cannot be found, there is a connection problem between the machine and the printer.

c To remove print jobs from the printer queue, type:

```
lprm ↵
```

Procedure 8-3 Problem: I discovered a new router, but cannot place it in a managed state

Possible causes are:

- an incorrect 5620 SAM server license key was entered or the license key is corrupt
- the 5620 SAM server license key is not for the correct hostid
- the number of cards (MDAs) managed exceeds the 5620 SAM server license key
- insufficient swap space for the 5620 SAM server
- another application is using a specific port required by the 5620 SAM server
- resychnronization problems between the managed network and the NMS domain

See Procedure 9-1 in chapter 9 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 router. See Procedure 9-5 in chapter 9 for more information.
- Failed deployment of the configuration request.

1 For the 5620 SAM client, perform the following:

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

The Deployment and Site Backup/Upgrade form with the Deployers tab button displayed appears. 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.

A deployment that is not sent to the managed devices means that the intended configuration change has not been made.

ii Choose a failed deployment and click on the Edit button to view additional information.

2 When a deployment has failed, and you have received 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 edit deployment form and contact your Alcatel support representative.

3 For client OSS applications, perform the following:

Note — These steps describe how to troubleshoot asynchronous deployment requests only. Alcatel 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 *Alcatel 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 *Alcatel 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 router failure, or by packet collisions caused by conflicting configurations from multiple sources. You can:

- resend the request
- troubleshoot your network or router

Procedure 8-5 Problem: I cannot find the backups of the router databases

Check the following:

- Device database backup settings have been set correctly.
- That .ndx and .cfg files have been created and saved to the router. See the *7750 SR OS System Guide* for more information.

1 To check that router database backup setting are correct from the 5620 SAM client, choose Choose Mediation→Deployment and Site Backup/Upgrade from the 5620 SAM main menu.

The Deployment and Site Backup/Upgrade form with the Deployers tab button displayed appears.

2 Click the Backup/Restore Policy tab button.

3 Verify the following parameter settings:

- Backup Mode
- FTP User Name
- FTP User Password
- Scheduled Backup Scheme
- Scheduled Backup Frequency
- Scheduled Backup Threshold (operations)
- CLI Config File Mode
- Boot Option File Mode
- Boot Option File Path
- 5620 SAM Server Repository Root Path

4 Modify the parameters settings if required.

5 Click the Apply button to save any changes.

6 Click the Backup/Restore Status tab button.

The devices are listed and backup and restore status information is displayed.

7 To view additional information, choose a device from the list and click the View button.

The Backup/Restore Manager form with the General tab button appears. Backup and Restore information is displayed. Click on the Backup Folders and the Faults tab buttons to view additional troubleshooting information.

Procedure 8-6 Problem: Cannot communicate with the 5620 SAM server

Check the following:

- The 5620 SAM client points to the correct IP address and port of the server.
- That the problem is not a network management domain LAN issue. See chapter 6 for more information.
- The server PC or workstation, or the server process on the PC or workstation, is not responding correctly, or is not running.

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 *install directory*/nms/config.

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 parameters if required.

5 Save the file if required.

6 To check server status, perform Procedure 9-4.

Procedure 8-7 Problem: Cannot start the client, or I get an error message when I start the client

Check the following:

- the 5620 SAM client and server have the same software versions and patch sets
- the login name and password of the user are correct
- the server is up
- the UNIX user of the 5620 SAM client has the same group permissions as the UNIX user who installed the 5620 SAM client.

1 To check that the 5620 SAM client and server versions are the same:

i Check the version of the 5620 SAM client by choosing Help→About from the 5620 SAM client GUI main menu.

The About form appears displaying the version of the 5620 SAM client.

ii Check the version of the 5620 SAM server in the server shell window. The shell can be viewed from the workstation on which the server is running.

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 Security→5620 SAM Security Manager from the 5620 SAM main menu.

The Security Management (Edit) form appears with the General tab button selected.

iii Click 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 Edit button.

The User 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 install 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.bat 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, peform Procedure 9-4.

Procedure 8-8 Problem: Problem collecting large numbers of logged statistics records or other large queries

When a client executes a request to the server to provide a large amount of data, such as requests for a large number of logged statistics, the 5620 SAM server may be unable to process the request if the query limit size is exceeded. A warning message is presented to the user on the client GUI, or an OSS client receives a SOAP invocation error indicating that the result set is too large. Modify the nms-server.xml file to change the limit.

1 Open the nms-server.xml file using a text editor. The default file location is *install directory*/nms/config

2 Change the externalQueyrLimit size parameter to an appropriate size. The parameter specifies the size of the queries allowed by the server when requested by a client.

3 The default number of records is 50000. Increase the number of records, for example, to 500000 for larger queries of logged statistics data.

Note — Increasing the limit consumes more server resources. A smaller limit is more suitable when multiple clients are requesting large amounts of data at the same time.

4 Save the changes to the file.

Procedure 8-9 Problem: Cannot view alarms from a 5620 SAM on a 5620 NM or 1354 BM

Possible causes include incorrectly configured param.cfg parameters on the 5620 NM or 1354 BM to allow the forwarding of alarms to those platforms from the 5620 SAM.

1 Open a command tool on the 5620 NM or 1354 BM.

2 For:

- **a** The 5620 NM, navigate to the AS tool IM directory by typing:

  ```
  /opt/netmgt/ALMAP/as/data/ascurim_0 ↵
  ```

- **b** The 1354 BM, navigate to the AS tool IM directory by typing:

  ```
  /usr/Systems/1354BMETH_1/AS/data/ascurim ↵
  ```

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.

For:

- **a** The 5620 NM, navigate to the AS tool IM configuration directory by typing:

  ```
  /opt/netmgt/ALMAP/as/data/ascurim_0/ASIMconfig ↵
  ```

- **b** The 1354 BM, navigate to the AS tool IM directory by typing:

  ```
  /usr/Systems/1354BMETH_1/AS/data/ascurim/ASIMFilter ↵
  ```

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 8-10 Problem: The GUI keeps shutting down

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

You can perform the following:

- from the 5620 SAM client GUI, admin users can disable the GUI inactivity check, if required.
- from the 5620 SAM client xml configuration file, reconfigure the client-server communication activity check to an appropriate time. The default is 1 min. The client and server communicate regularly to determine if a session is still active. If the communication fails during the specified time, the session is stopped. Causes for the failure could be heavy server or network traffic.

1 To disable the GUI activity check, choose Security→5620 SAM Security Manager from the 5620 SAM main menu.

The Security Management (Edit) form appears with the General tab button 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 shutdown due to inactivity.

3 Save the changes and close the form.

4 To reconfigure the reconfigure the client-server communication activity check.

i Open the nms-client.xml file using a text editor. The default file location is *install directory*/nms/config

ii Change the serverTimeoutMinutes parameter to an appropriate time. The parameter specifies the amount of time that can elapse without client-server communication. The client shuts down when the time elapses if activity checking is enabled.

iii Save the file.

5 Changes to the configuration of the server may cause communication problems and eventually lead to the server shutting down.

a Check for the server heartbeat in the status bar of the client GUI. If the heartbeat disappears, check LAN communication between the server and client. See chapter 6 for more information about network management LAN troubleshooting.

b Changing the operating system system clock on the server PC or workstation can cause communication problems on the client. If the server system clock is changed, the clients should log off and the server should be restarted. Alcatel recommends that the server system clock should be tied to a synchronous timing source, to eliminate time shifts that may lead to polling and communication problems.

Procedure 8-11 Problem: I saved a configuration on the GUI, but cannot see the change

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 main configuration form is saved. For example, when you configure a VLL service, sites or L2 interfaces that you have configured are not saved until the service is created when the main 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 that indicates when objects that have been configured in contained configuration forms will not be saved until parent configuration forms are saved.

Procedure 8-12 Problem: I performed a search or list function, and it takes too long to complete

You can perform simple or complex searches using the Find menu on the 5620 SAM main menu to query the database for information about services, subscribers, and other stored data. When you use a simple search to display, at the same time, the following types and numbers of objects, performance may be affected. Use a filtered search to reduce the number of objects.

- more than 5 000 services and more than 5 000 services for subscribers
- more than 10 000 FIB or ACL entries

Procedure 8-13 Problem: I cannot select certain menu options or I cannot save 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 privileges.

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 8-14 Problem: I cannot see related object information for an alarm

The 5620 SAM limits the propagation of relationships related to alarms information when the number of alarms in the database exceeds 10, 000. These relationships are used to perform alarm correlation. Should alarm correlation be necessary, the administrator can increase the alarm count. The alarm count should not be increased if GUI performance is affected by the number of outstanding alarms. Reduce the number of outstanding alarms by logging alarms whenever possible.

1 Go to the *install directory*/nms/config directory or folder on the server and locate the nms-server.xml file.

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

3 Search for the <faultManager maxAlarmCount="*XXX*"> tag.

4 Modify the value, as required.

5 Save the changes and close the file.

6 From the install directory/nms/bin directory or folder on the server machine, run the following

```
nmsserver read_config ↵
```

This reconfigures the maximum alarm count on the server.

Procedure 8-15 Problem: I cannot clear alarms using the 5620 SAM client GUI

A resynchronization problem between the 5620 SAM client GUI and the server/network may cause alarm clearing issues. Try the following:

- resynchronize the managed devices
- stop and restart the client GUI
- check server status
- check the SNMP trap destination from the managed devices

1 Try the following:

a Resynchronize the devices:

i Choose Mediation→Discovery Manager from the client GUI main menu.

ii Click on the Resync Status tab button.

iii Select a device.

iv Choose to ignore timestamps.

v Click on the Resync button.

b Stop and start the client GUI, as described in the *5620 SAM User Guide*.

c Run the nmsserver status script, as described in Procedure 9-4. Check that sufficient free memory is available.

d Check the destination of SNMP traps from the managed devices, as configured using the *5620 SAM Installation and Upgrade Guide*. If necessary, ping the management IP address of the 5620 SAM server to ensure IP reachability from the managed devices. Devices can appear to be managed from the client GUI even if there is no IP reachabiltiy, but resynchronizations will fail in that case.

2 Collect the EmsServerLog and EmsClientLog files for your Alcatel support representative, as described in chapter 2.

Procedure 8-16 Problem: Received an exception that an SSL PKI certificate is not trusted

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 nmsclient.bat 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

9 — Troubleshooting 5620 SAM server issues

9.1 Troubleshooting 5620 SAM server issues

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

Procedure 9-1 Problem: Cannot manage new routers or cannot launch the 5620 SAM 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.
- 5620 SAM-O cannot connect because the license key is not enabled for 5620 SAM-O
- Swap space is insufficient.
- 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 in the *install directory*/nms/config nms-server.xml file.

1 Check the license key.

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

The About form appears.

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 *install 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>. The license key indicates the following:

- the version of the software and the version of the license key match
- the total number of cards (MDAs) managed is within the license key limit
- the availability of the 5620 SAM-O server
- the customerName and host ID match the value provided when the license key was issued
- the software modules that are installed and licensed, which determines the type of functionality available using the client GUI

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

vi Type the updated license key in the file, if required.

vii Save the changes, if required.

viii Open a shell or window.

ix Go to the *install directory* bin directory or folder.

x Type:

```
nmsserver 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 Check the amount of swap space available. Insufficient swap space can prevent the 5620 SAM server from launching. See Procedure 7-4 for more information.

3 Specific ports need to be available for the 5620 SAM server. See Procedure 6-4 for more information about specific port values.

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

ii Check the ejbServerPort xml tag.

iii Ensure that this port number is not used by any other application. For example, a browser launched on the same platform as the 5620 SAM server may be using the same port number required by the 5620 SAM server. Alcatel recommends that you do not run any other applications on the 5620 SAM server platform.

4 The 7450 ESS and 7750 SR are configured to send SNMP packets of up to 9216 bytes, as described in step 3 in Procedure 9-3.

When an intermediate network device, such as a router, receives the management traffic to and from the 5620 SAM and the managed network, it must be able to process packets of up to 9216 bytes. If this exceeds the MTU for the intermediate device, or if the device cannot perform packet fragmentation, then large packets may be dropped and resynchronization may fail. Consider the following:

- Ensure devices located between the managed devices, such as the 7750 SR, and 5620 SAM can handle an MTU size of 9216 bytes or can fragment large SNMP packets.
- 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, using a large packet.
- Ensure firewalls between the 7450 ESS and 7750 SR and the 5620 SAM sever are configured to allow traceroute and ping packets.

i Log on to the 7750 SR or other 5620 SAM-managed device.

ii Run the traceroute command:

```
> traceroute SAM_server_IP_address ↵
```

A list of hops and IP addresses appears.

iii 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 packet size or packet fragmentation.

iv Repeat for all other hops until a ping fails, or until a message indicates that there is an MTU mismatch. When a ping fails, it indicates that the intermediate device does not support large SNMP packets or packet fragmentation.

v Check the configuration of the intermediate device, and configure fragmentation or enabled a larger MTU size.

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

When the links and 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. The ping -s command issues a number of sequentially ordered packets. If these packets are returned out of sequence, it indicates that there are LAN problems.

1 Perform a ping -s to test reachability, as described in Procedure 6-3.

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: 5620 SAM server response times are slower than normal

As the number of managed devices grows and when more GUI or OSS clients are brought online, the processing load on the 5620 SAM server increases. Ensure the following:

- minimum platform requirements for the 5620 SAM server are met
- server performance is fine-tuned to allow for network growth

1 Verify the minimum platform requirements for your system. See the appropriate release notice or the platform sizing document, available from your Alcatel support representative.

2 Try to ping -s the server, as described in Procedure 9-2.

3 Check that the engine ID for the managed device has not been reused by multiple managed devices, as described in Procedure 9-6.

4 Fine-tune the number of threads that are available to handle general deployment requests from the clients to the network and the threads that are available to handle statistics collection from network devices.

i Go to the *install directory*/nms/config directory.

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

iii Search for the following text: deploymentWorker.

iv Update the number of threads available. The range is 1 to 30. The default is 10.

- The nePoolSize specifies the number of deployment threads. Increase the number, depending on the increase in the amount of client configuration activity, or the number of network devices.
- The statsPoolSize specifies the number of statistics collection threads. Increase the number, depending on the increase in the interval and number of statistics collected from network devices, or the number of devices from which statistics are collected.

v Save the changes and close the file.

Procedure 9-4 Problem: Unsure of the status of my server

The server executable provides flags that can be used to determine the status of the server, including the following:

- how long the server has been up
- memory available and used
- database connectivity status
- threads in use

1 Open a shell or window.

2 Go to the *install directory* bin directory or folder.

3 Launch the nmsserver.bash or nmsserver.bat executable with the following flag:

```
nmsserver.* executable flag ↵
```

where

*nmsserver.** is either nmsserver.bash or nmsserver.bat

executable flag is one of the options in Table 9-1

Table 9-1 nmsserver.* flag options

Flag option	Description
daemon	Starts the 5620 SAM server in non-interactive mode. This is the recommended usage. Not using a flag also starts the server in interactive mode.
start	Starts the 5620 SAM server in interactive mode.
appserver_status	Provides information about the status of the 5620 SAM server. See step 4 for more information.
appserver_version	Provides build information, including the start date of the current instance of the 5620 SAM server.
nms_status *username userpassword*	Provides the following information: • 5620 SAM server start time and running time • total available memory and memory used • status of a database connectivity test • number and status of memory threads in use
nms_version	Provides the current build of 5620 SAM software.
jvm_version	Provides information about the currently running version of the Java Virtual Machine environment.
read_config	Provides the ability to reread the server configuration file, nms-server.xml, while the server is running. This allows you to update parameters for the server without shutting the server down, for example, to update alarm agent settings or change the managed card (MDA) license count.
script_env	Provides information about the directory structure of scripts used by the 5620 SAM software.
stop	Stops the 5620 SAM server.

4 The following sample shows the output of the appserver_status option. This option provides general information about the server. It also lists thread information.

```
Application Server is started

-----------------------------

HostAddress=138.120.152.74

AvailableProcessors=2

OSArch=sparc

OSVersion=5.9

HostName=mojo

JavaVendor=Sun Microsystems Inc.

JavaVMName=Java HotSpot(TM) Client VM

FreeMemory=902843456

ActiveThreadGroupCount=5

TotalMemory=1255145472

JavaVMVersion=1.4.2_02-b03

ActiveThreadCount=145

JavaVMVendor=Sun Microsystems Inc.

OSName=SunOS

JavaVersion=1.4.2_02

MaxMemory=1255145472

#
```

5 Check the output to ensure the following:

- free memory falls within the available memory range, with memory to spare
- the MaxMemory and TotalMemory values match or are close in value, otherwise other applications may be affecting available memory for use by the 5620 SAM applications
- the number of available processors matches your hardware specifications, otherwise not all processors may be working properly

Procedure 9-5 Problem: All SNMP traps from 7750 SRs are arriving at one 5620 SAM server, or no SNMP traps are arriving

When you install the 5620 SAM server, you specify a port where SNMP traps arrive. In addition, two sets of configurations must be completed for SNMP trap notifications to work:

- Enable key SNMP parameters on the routers 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 group and user permissions to configure the managed devices.

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

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

```
configure router interface system
```

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

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

ii Close CLI.

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

```
configure system snmp no shutdown
```

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

where *name of community* is the SNMPv2 community name

```
admin save
```

Note — The command is used for the 5620 SAM write mediation policy. If you are using SNMPv2, you must use this mediation policy for read as well, or create another mediation policy that is also configured for rwa.

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

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

```
admin save
```

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

```
bof

persist on

save

back

admin save

admin synchronize boot-env

admin reboot

Are you sure you want to reboot? (y/n) y
```

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

5 Run the following CLI command to enable Telnet on the managed device. By default, the devices use SSH:

```
config system security telnet-server
```

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

```
configure log

info
```

Check the output for the following information.

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

7 Go to the *install directory*/nms/config directory or folder to check that SNMP values are correctly set to enable traps to reach the 5620 SAM server.

8 Open the nms-server.xml key file using a text editor. Search on the tag <snmp>.

9 Verify the following:

- the port is available to the network devices
- the trapLogId is unique for each network device to communicate with the 5620 SAM

10 Update the <snmp> fields as required.

11 Save the changes, if required, and close the file.

Procedure 9-6 Problem: Cannot discover more than one device or a resynchronization of devices fails

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

1 Verify the engine IDs in the managed network using the client GUI and CLI on all managed devices. See the *5620 SAM User Guide* and the appropriate device documentation for more information.

2 If required, use CLI to change the change the engine ID. See the appropriate device documentation for more information.

3 Configure or modify the configuration of SNMPv3. See the *5620 SAM User Guide* for more information.

4 If required, check the NIC card and all cables from the managed devices to the network management domain. This problem may be seen when numerous Poller Problem communication alarms are raised.

Procedure 9-7 Problem: The 5620 SAM server starts up, and then quickly shuts down

Redirect the output of the nmsserver startup to check for JVM errors.

1 Open a command tool or DOS prompt.

2 Before you start nmsserver.bat or nmsserver.bash, output the startup messages to a readable console by typing:

```
nmsserver.bat > server.out log 2/&1
```

where *server.out* is the log file name

3 Review the log output for JVM process errors.

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 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: Communication issues between the 5620 SAM server and database

Check the following:

- ensure that you can ping the database 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 6-4

1 Go to the *install directory*/nms/config directory or folder and locate the nms-server.xml file to check that database values are set correctly to allow the 5620 SAM server to communicate with the database.

i Open the nms-server.xml key file using a text editor. Search on the tag <db>.

ii Verify the following:

- the port number indicated is available between the server and the database
- the correct database host IP address is indicated
- the database name, database username, and password match the names configured during installation, as described in the *5620 SAM Installation and Upgrade Guide*

iii Save the changes, if required, and close the file.

2 Go to the *install directory*/nms/config directory or folder and locate the nms-server.xml file to check that redundant database configuration values are set correctly to allow the 5620 SAM server to communicate with the active database and, in the case of a database failure, the standby database.

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

ii Verify the following:

- To allow automatic failover between the active and standby databases, ensure the allowFailOver parameter is set to yes. The default is no.
- To allow manual switchovers between the active and standby databases using the client GUI, ensure the allowSwitchOver parameter is set to yes.
- To specify the number of database connection retries initiated by the server before a failover to the standby database is performed, ensure the dbConnectMaxRetries parameter is configured.
- The database name, database username, standby database name, standbyHost, primaryTnsName, standbyTnsName, and passwords match the settings configured during installation, as described in the *5620 SAM Installation and Upgrade Guide*.

iii Save the changes, if required, and close the file.

Procedure 9-10 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 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, and the user logged into the 5620 SAM must have FTP permissions on the managed device, as specified in the *5620 SAM User Guide*

Alcatel 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 and the polling ratio are configured sufficiently for the statistics you are polling in the MIB and MIB entries

Procedure 9-11 Problem: Redundancy issues for the 5620 SAM server and database

Check:

- that all parameters configured using the DBconfig and ClientServerInstall installers were performed correctly, as described in the *5620 SAM Installation and Upgrade Guide*
- that there is sufficient time for the server to validate the need for an activity check
- configurations are correct to handle two redundant servers behind a firewall

1 Go to the *install directory*/nms/config directory or folder and locate the nms-server.xml file to check that redundant database configuration values are set correctly to allow the 5620 SAM server to communicate with the primary (active) database and, in the case of a database failure, the standby database.

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

ii Verify the following:

- To allow redundancy, ensure the redundancyEnabled parameter is set to true.
- To ensure proper communication of TCP messages from the server to the database about failover and switchover messages, ensure that TCP port 9002 is available and open.
- To allow manual switchovers between the active and standby databases using the client GUI, ensure the allowSwitchOver parameter is set to yes.
- To allow manual failovers between the active and standby databases using the client GUI, ensure the allowFailOver parameter is set to yes.
- To allow automatic failovers between the active and standby databases using the client GUI, ensure the dbAutoFailOver parameter is set to yes.
- To specify the number of database connection retries initiated by the server before a failover to the standby database is performed, ensure the dbConnectMaxRetries parameter is configured. The default is 100.
- The database name, database username, standby database name, standbyHost, and passwords match the settings configured during installation, as described in the *5620 SAM Installation and Upgrade Guide*.

2 Save the changes, if required, and close the file.

3 The detection failure check default time for primary to standby server pings should be sufficient in most network cases. However, when there are dropped packets in the NMS LAN, the server redundancy check timeout value should be changed to ensure LAN problems do not cause a server activity switch.

i As admin, open a command or shell tool.

ii Change to the *install_dir*/nms/jboss/server/default/deploy directory

iii Open the cluster-service.xml file using an editor.

iv Change the ping timeout value. The default value is 1500 ms, and the server tries to verify connectivity three times. By default, the activity switch occurs (3 X *timeout_value*) + *timeout_value*)).

v Save the changes and close the file.

4 Check firewall configurations, and ensure that the cluster-service.xml file in the /nms/jboss/server/default/deploy directory is properly configured, as indicated in the *Alcatel 5620 SAM Planning Guide*.

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 nmsserver.bat or .bash 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 *.bash 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 *.bash 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
```

10 — Troubleshooting the 5620 SAM database

10.1 Database troubleshooting

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

Warning — Performing any database modifications using the Oracle database or tablespace tools can cause irreparable harm to the database and your network management data. Performing such modifications can void your Alcatel warranty and support agreements. Contact your Alcatel technical support representative to help you troubleshoot your database.

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 archived 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 support representative.

2 Check the partition or root database backup directory to ensure that:

- the size of the assigned disk space or slice is sufficient
- the disk directory or slice is sufficient to hold the three database backups in the backupset1, backupset2, and backupset3 folders or directories

3 If the disk directory has many archived log files due to underscheduling of database backups:

i Locate the archived log files on the database PC or workstation.

ii Delete the files using an appropriate operating system utility.

iii Connect to the RMAN Oracle utility to indicate the archived log file deletion by typing:

```
rman target user_name/user_password ↵
```

where *user_name* and *user_password* are the Oracle database user account and password

iv Type the following commands to verify the archivelog changes and to exit RMAN:

```
RMAN>crosscheck archivelog all; ↵
```

```
RMAN>exit; ↵
```

v Perform a database backup using the 5620 SAM client GUI, as described in the *5620 SAM User Guide*, or using the DBconfig installer, as described in the *5620 SAM Installation and Upgrade Guide*.

vi 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 its system resources to create the backups.

1 On a 5620 SAM client GUI, choose Policies→Database Manager 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 Frequency and Frequency Unit parameters. For example, setting the Backup Frequency parameter to 6 and setting the Frequency 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 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, overwritten, and has enough space to contain the database. For regularly scheduled backups, ensure that there is enough space for numerous backup copies of the database.

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. Alcatel recommends that the database is restored on a new workstation. If you must 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 any database modifications using the Oracle database or tablespace tools can cause irreparable harm to the database and your network management data. Performing such modifications can void your Alcatel warranty and support agreements. Contact your Alcatel technical support representative to help you troubleshoot your database.

1 As the oracle user, launch the 5620 SAM database configuration tool from the appropriate directory on the product DVD, as described in the *5620 SAM Installation and Upgrade Guide*.

a For Solaris, type:

```
./DBConfig.bin ↵
```

b For Windows, double-click on the DBconfig.exe file.

The 5620 SAM database configuration tool is launched.

2 Specify the following database restore information, which is available from the dbconfig.properties file or the Policies→Database Manager 5620 SAM client GUI main menu:

- database name
- DBID, which is the unique numerical identifier of the database as shown in the control file backup, after the 'c-' prefix. For example, for c-123456789-20050505-00 the DBID is 123456789.
- database instance name, which must be unique if the database restore is performed on the same workstation where the original database is installed, and the original database is not removed

Note — If you use an existing database instance name for the new database instance name, the existing database instance is overwritten.

3 Specify the backup directory where the backed up version of the database can be found.

The path to the backup directory on the restoration workstation must match the backup directory on the workstation where the backup is made.

4 Specify whether to create a copy of the backed up database. When the backup database is restored, Oracle modifies the backup and it cannot be reused.

5 Specify any additional parameters, as listed in the *5620 SAM Installation and Upgrade Guide*.

6 For Solaris installations, run the following from the *install directory*/config/*databasename* directory:

`solaris_root.sh` ↵

This script enables automatic database startup and shutdown at reboot.

To retrieve the changes since the database was saved and restored, you can:

- wait for the normally scheduled polling interval to retrieve the latest changes to the MIB
- resync with the network
- rediscover portions of the network as required

Procedure 10-4 Problem: The Oracle database is not performing as expected on a Solaris platform

Warning — Performing any database modifications using the Oracle database or tablespace tools can cause irreparable harm to the database and your network management data. Performing such modifications can void your Alcatel warranty and support agreements. Contact your Alcatel technical support representative to help you troubleshoot your database.

1 Ensure that the following Solaris kernel settings are correct in the /etc/system file:

```
set semsys:seminfo_semmni=100
set semsys:seminfo_semmns=1024
set semsys:seminfo_semmsl=256
set semsys:seminfo_semmnu=400
set semsys:seminfo_semume=200
set shmsys:shminfo_shmmax=value_of_RAM
set shmsys:shminfo_shmmin=1
set shmsys:shminfo_shmmni=100
set shmsys:shminfo_shmseg=10
```

where *value_of_RAM* is at least half of physical RAM size for the workstation platform, for example 1073741824 for 2Gbytes of RAM

2 Ensure the shmmax value in the system file does not exceed available physical RAM.

3 Reboot the system using the init 6 command.

Caution — Failure to reboot may cause Oracle database problems.

Procedure 10-5 Problem: The database restore fails with a no backupsets error

Warning — Performing any database modifications using the Oracle database management tools can cause irreparable harm to the database and your network management data. Performing such modifications can void your Alcatel warranty and support agreements. Contact your Alcatel technical support representative to help you troubleshoot your database.

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.

Use the following procedure to change the status of database backupsets from expired to available. Before you perform this procedure:

- the control file must be restored
- the database instance must be started, but not mounted, using the restored control file

1 On the restore server, connect to the target database using RMAN by typing:

```
rman target user_name/user_password ↵
```

where *user_name* and *user_password* are the Oracle database user account and password

See the appropriate Oracle documentation for more information about using RMAN.

2 List all database backupsets by typing:

```
RMAN>list backup; ↵
```

3 Record the numbers of the database backupsets that are marked as expired.

4 Change the status of the expired database backupsets to available by typing:

```
RMAN>change backupset backupset_number available; ↵
```

where *backupset_number* is the database backupset that you want to set to available and restore

5 List all database backupsets listed in step 2 and verify that the status of the required backupset is set to available.

6 Restore the database using RMAN command by typing:

```
RMAN>restore database; ↵

RMAN>recover database; ↵

RMAN>alter database open resetlogs; ↵
```

Procedure 10-6 Problem: database redundancy is not working

Warning — Performing any database modifications using the Oracle database management tools can cause irreparable harm to the database and your network management data. Performing such modifications can void your Alcatel warranty and support agreements. Contact your Alcatel technical support representative to help you troubleshoot your database.

Database redundancy between an primary (active) and standby is performed during installation.

1 Ensure that database redundancy configuration was performed properly, as specified in the *5620 SAM Installation and Upgrade Guide*:

- The primary database was configured before the standby database.
- The primary and standby databases must be on different workstations.
- Ensure the active and standby database directory structures and configurations are identical on both workstations.
- Ensure that there are identical operating system and versions of the 5620 SAM software installed on the active and standby database workstations.

2 Ensure there are no LAN communication problems between the active and standby database platforms. Consult your LAN troubleshooting guidelines, or chapter 6 for more information.

3 Ensure the database redundancy parameters are properly configured in the 5620 SAM server nms-server.xml file. See Procedure 9-11.

Procedure 10-7 Problem: unable to verify that Oracle database and Listener services have 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 database configuration was performed properly, as specified in the *5620 SAM Installation and Upgrade Guide*

2 To verify that Oracle Listener and Oracle database services have started.

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:

i For the Listener, type:

```
ps -ef|grep tnslsnr ↵
```

One entry should be shown for the Listener.

ii For the database, type:

```
ps -ef|grep ora ↵
```

There should be multiple Oracle instances listed.

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:

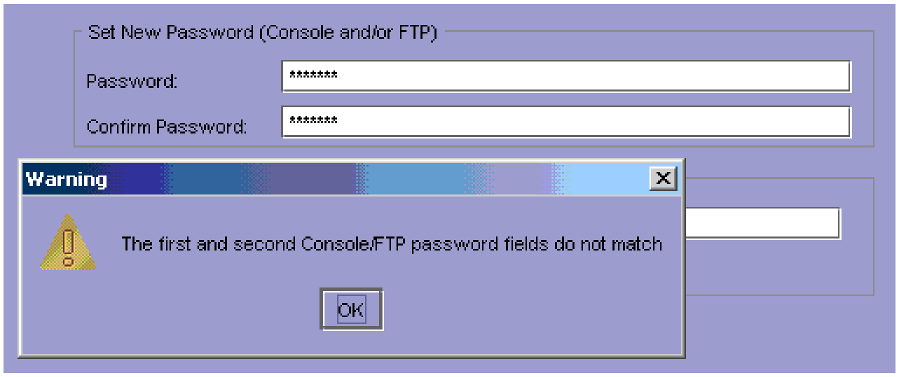
- information has been entered incorrectly
- additional information is required
- the operation you are attempting cannot be completed
- a change to a configuration sub-form will not be committed until the parent form is committed
- an operation that may result in service disruption is requested
- a 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.

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



Set New Password (Console and/or FTP)

Password: *******

Confirm Password: *******

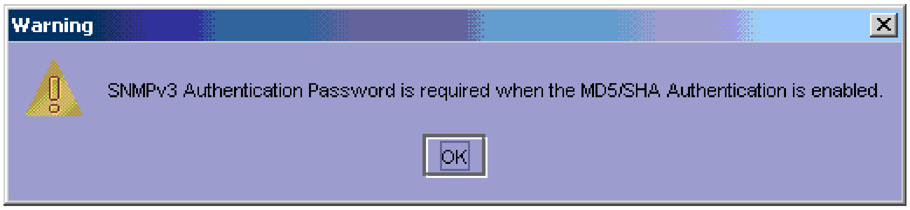
Warning

The first and second Console/FTP password fields do not match

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



SNMPv3 Authentication Password is required when the MD5/SHA Authentication is enabled.

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

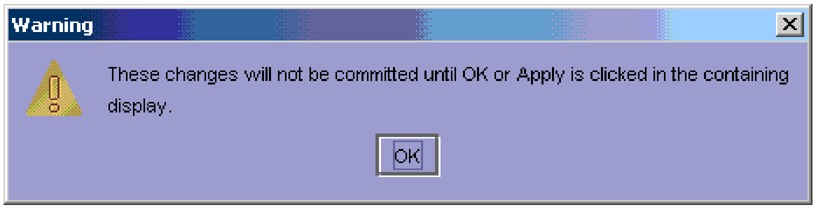
Warning messages are used to indicate that a specific action cannot be completed. These warnings may occur when you try to create a new object or modify an existing object that results in an unsupported configuration. For example, the message “Can't bind LSP to a non-mpls service tunnel“ indicates that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

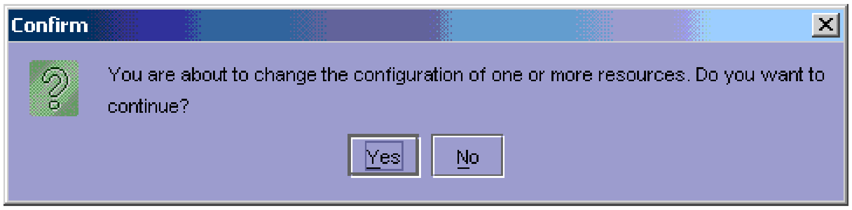
Figure 11-3 Committing changes warning dialog box



These changes will not be committed until OK or Apply is clicked in the containing display.

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



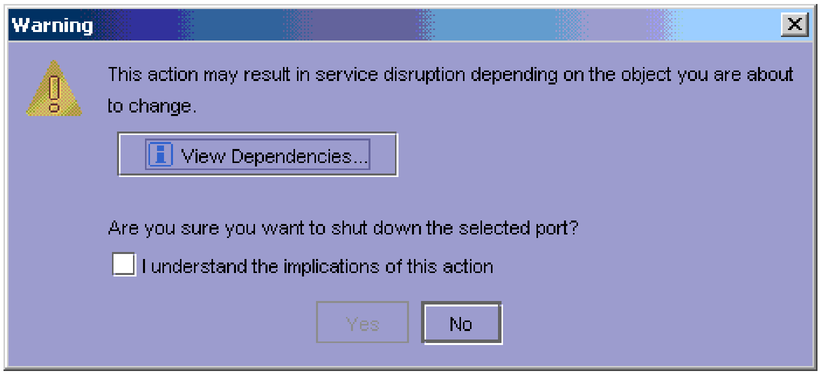
You are about to change the configuration of one or more resources. Do you want to continue?

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



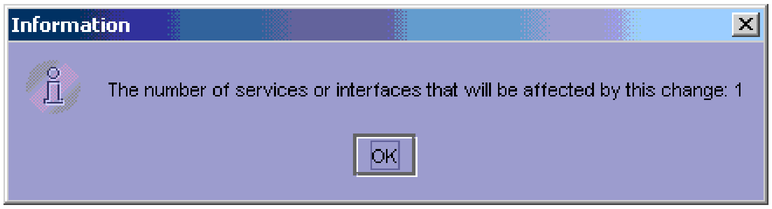
This action may result in service disruption depending on the object you are about to change.

Are you sure you want to shut down the selected port?

□ I understand the implications of this action

As indicated by the warning message, the action you are about to perform may cause a disruption to subscriber 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



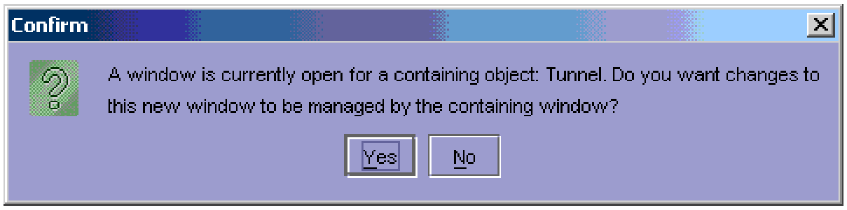
The number of services or interfaces that will be affected by this change: 1

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 service by choosing Service Management→Browse Services, or you can access the service by clicking on the Services tab button for a specified subscriber after you choose Service Management Manager→Subscribers/Services. 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



Confirm

A window is currently open for a containing object: Tunnel. Do you want changes to this new window to be managed by the containing window?

When this warning message is displayed, you have another form 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

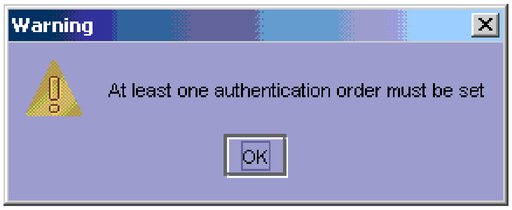
The following procedure describes how to respond to a warning message when you perform an action with the 5620 SAM client.

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



Warning

At least one authentication order must be set

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:

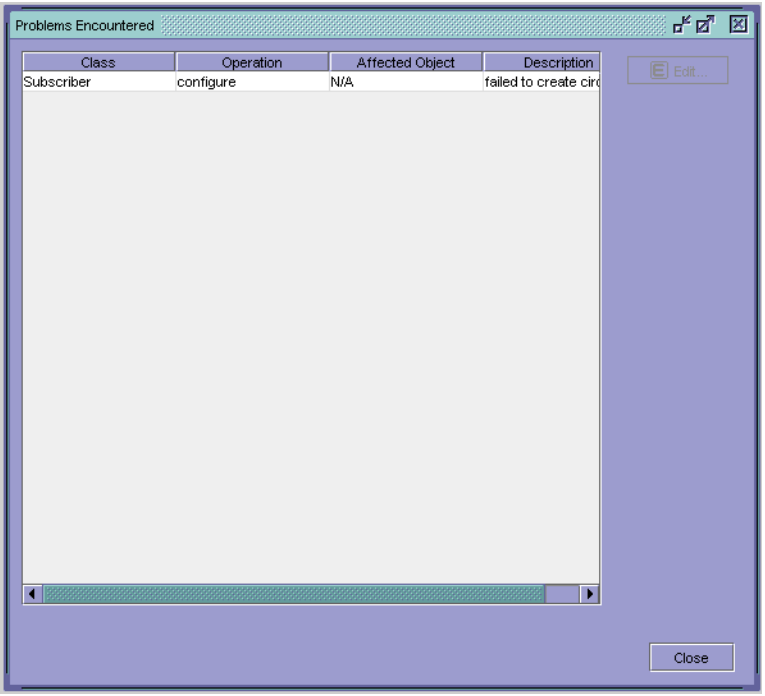
- **a** Check the documentation to ensure that you are following the steps correctly.
- **b** Verify that you are trying to perform an action that is supported.
- **c** Review the general troubleshooting information in section 1.3.
- **d** If you cannot resolve the problem, perform Procedure 2-1 before 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



Problems Encountered

Class	Operation	Affected Object	Description
Subscriber	configure	N/A	failed to create circ

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 Edit 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

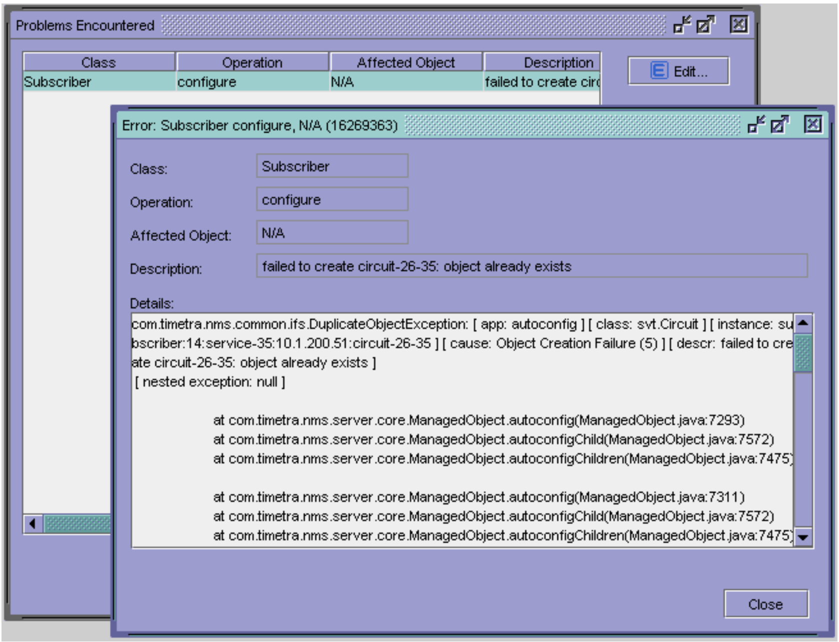
The following procedures describe how to view additional information about a problem in a Problems Encountered form and the information to collect before you contact your technical support representative.

Procedure 12-1 To view additional problem information

1 Choose an entry in the Problems Encountered form.

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

Figure 12-2 Problems Encountered form details



Class	Operation	Affected Object	Description
Subscriber	configure	N/A	failed to create circ

Class: Subscriber

Operation: configure

Affected Object: N/A

Description: failed to create circuit-26-35: object already exists

Details:

```
com.timetra.nms.common.ifs.DuplicateObjectException: [ app: autoconfig ] [ class: svt.Circuit ] [ instance: su
bscriber:14:service-35:10.1.200.51:circuit-26-35 ] [ cause: Object Creation Failure (5) ] [ descr: failed to cre
ate circuit-26-35: object already exists ]
 [ nested exception: null ]

            at com.timetra.nms.server.core.ManagedObject.autoconfig(ManagedObject.java:7293)
            at com.timetra.nms.server.core.ManagedObject.autoconfigChild(ManagedObject.java:7572)
            at com.timetra.nms.server.core.ManagedObject.autoconfigChildren(ManagedObject.java:7475)

            at com.timetra.nms.server.core.ManagedObject.autoconfig(ManagedObject.java:7311)
            at com.timetra.nms.server.core.ManagedObject.autoconfigChild(ManagedObject.java:7572)
            at com.timetra.nms.server.core.ManagedObject.autoconfigChildren(ManagedObject.java:7475)
```

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 support

The following procedure describes what to do before you contact your contact 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 the following:

- nms-client.xml file from the *install directory*/nms/config directory or folder.
- server logs, for example, the EmsServerLog.txt file from the *install directory*/nms/log directory or folder
- client logs, for example, the EmsClientLog.txt file from the *install directory*/nsm/log directory

  The same information that appears in the Problems Encountered form details is also written to the client log file and the server log file depending on the condition that caused the problem.

Note — Log files are generally overwritten when systems are restarted. Some long-running applications can generate multiple log files. Most log files are stored in the *install_directory*/version/nms/log directory or folder.

5 Store the files in a secure location.

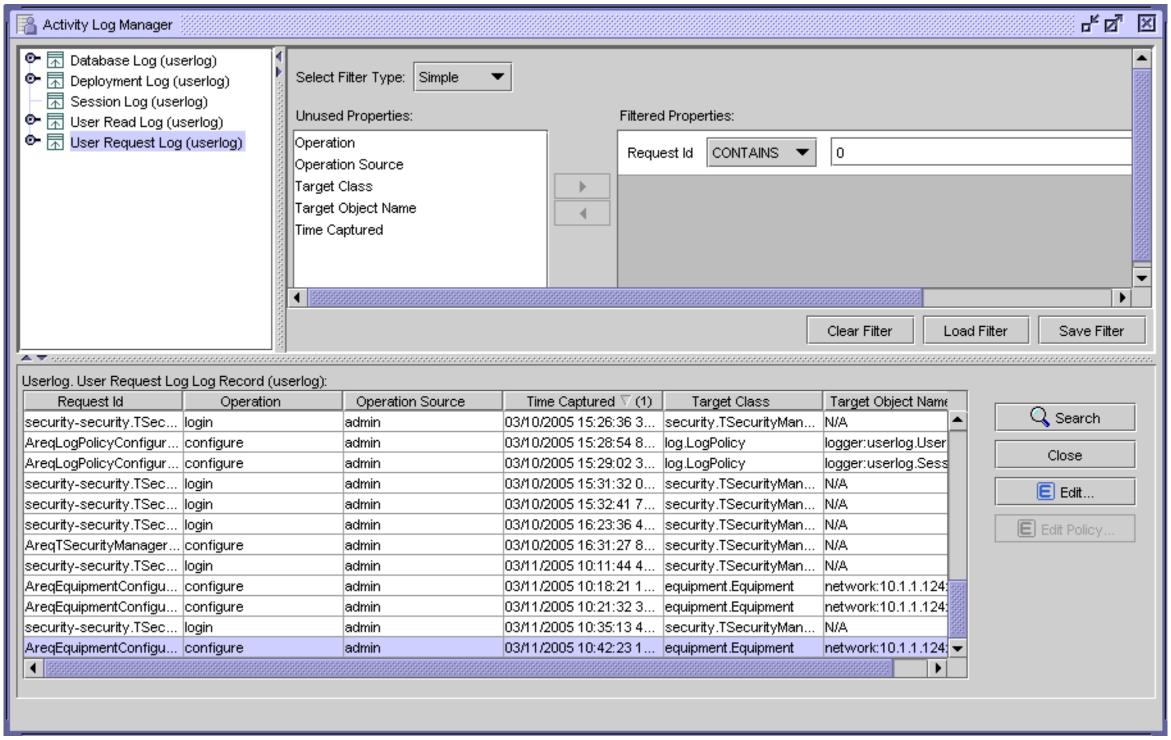
6 Send the information collected to your technical support representative.

13 — Troubleshooting with the client activity log

13.1 Activity Log Manager form overview

The Activity Log Manager allows users with administrative privileges to view user activity for 5620 SAM GUI and OSS clients. Figure 13-1 shows the Activity Log Manager form.

Figure 13-1 Activity Log Manager form details



Select Filter Type: Simple

Unused Properties:

Operation
Operation Source
Target Class
Target Object Name
Time Captured

Filtered Properties:

Request Id CONTAINS 0

Userlog. User Request Log Log Record (userlog):

Request Id	Operation	Operation Source	Time Captured ▽ (1)	Target Class	Target Object Name
security-security.TSec...	login	admin	03/10/2005 15:26:36 3...	security.TSecurityMan...	N/A
AreqLogPolicyConfigur...	configure	admin	03/10/2005 15:28:54 8...	log.LogPolicy	logger:userlog.User
AreqLogPolicyConfigur...	configure	admin	03/10/2005 15:29:02 3...	log.LogPolicy	logger:userlog.Sess
security-security.TSec...	login	admin	03/10/2005 15:31:32 0...	security.TSecurityMan...	N/A
security-security.TSec...	login	admin	03/10/2005 15:32:41 7...	security.TSecurityMan...	N/A
security-security.TSec...	login	admin	03/10/2005 16:23:36 4...	security.TSecurityMan...	N/A
AreqTSecurityManager...	configure	admin	03/10/2005 16:31:27 8...	security.TSecurityMan...	N/A
security-security.TSec...	login	admin	03/11/2005 10:11:44 4...	security.TSecurityMan...	N/A
AreqEquipmentConfigu...	configure	admin	03/11/2005 10:18:21 1...	equipment.Equipment	network:10.1.1.124
AreqEquipmentConfigu...	configure	admin	03/11/2005 10:21:32 3...	equipment.Equipment	network:10.1.1.124
security-security.TSec...	login	admin	03/11/2005 10:35:13 4...	security.TSecurityMan...	N/A
AreqEquipmentConfigu...	configure	admin	03/11/2005 10:42:23 1...	equipment.Equipment	network:10.1.1.124

Table 13-1 describes the types of logs available in the Activity Log Manager form.

Table 13-1 Log types available in the Activity Log Manager 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 *Alcatel 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
- object that was the target of the operation
- execution status of the operation

Note — You must manually refresh the display in the Activity Manager Log 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.

Note — Administrative operators can independently enable and disable each activity log. See the *5620 SAM User Guide* for information on how to enable and configure the activity logs associated with the Activity Log Manager form.

Table 13-2 lists the log file entries for select 5620 SAM actions.

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 Activity Log Manager forms

The following procedures describe how to use the Activity Log Manager form to correlate user requests and deployment activity.

Procedure 13-1 To identify the user associated with a network problem

1. Click on the Deployment Log (userlog) entry in the Activity Log Manager form.
2. Select the filter properties for the log display, if required.
3. Click on the Search button. A list of deployment log activity appears.

4 Identify the network problem by reviewing the status of the Result column. There is no check mark in the Result column for failed deployments.

5 Identify and record the request ID for the failed deployment using the Request Id column.

6 Click on the User Request Log (userlog) entry in the Activity Log Manager form.

7 Use the filter in the User Request Log (userlog) to list the requests for the request ID that you obtained in step 5. 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 Click on the User Request Log (userlog) entry in the Activity Log Manager form.

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 the Database Log (userlog) entry in the Activity Log Manager form.

6 Use the filter in the Database Log (userlog) to list the database activity associated with the request ID that you obtained in step 4. 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 Click on the User Request Log (userlog) entry in the Activity Log Manager form.

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 the Deployment Log (userlog) entry in the Activity Log Manager 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 filter results in the Userlog display area.

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 failed deployments.

Procedure 13-4 To retrieve historical user logs

1 Choose Find→Browse Log Records from the 5620 SAM main menu. The Browse Log Records form appears.

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 Edit button. The logger form for the selected user log appears.

5 Click on the View History button. The Browse 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 by most recent.

b Click on the Target Class column heading to sort the records by the type of object against which the user log was generated.

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 SAM 5620 Service Aware Manager

The 5620 SAM is the network manager portfolio of modules for the 7750 SR and 7450 ESS.

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

5620 SAM database The 5620 SAM database stores network objects and configurations.

5620 SAM server The 5620 SAM server mediates between the 5620 SAM database, 5620 SAM client, and the network.

5620 SAM-A 5620 SAM Assurance

The 5620 SAM-A provides service assurance functionality.

5620 SAM-E 5620 SAM Element Manager

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

5620 SAM-O Alcatel 5620 SAM Open Interfaces

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

5620 SAM-P Alcatel 5620 SAM Provisioning

The 5620 SAM-P provides service provisioning functionality.

A

alarm

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

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

C

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.

CPE

customer premises equipment

Network equipment that resides on the customer's premises.

CPU

central processing unit

F

fault

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

FTP

file transfer protocol

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

G

GUI

graphical user interface

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

I

IETF

Internet engineering task force

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

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.

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

L

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.

M

MDA

media dependent adapter

menu bar

The menu bar is a tool on the GUI that organizes tasks across broad headings. You can perform functions on the application by selecting an action from the menu bar.

MIB

management information base

MTU

maximum transmission unit

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

N

navigation tree

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

NE

network element

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

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

networkstation A UNIX platform where the 5620 SAM software runs.

NPDU network protocol data unit

O

OSS operational support system

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

P

PC personal computer

PDU protocol data unit

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

Q

QoS Quality of Service

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

R

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.

routing instance A routing instance is the configuration of a router, including information such as protocols, interfaces, routing, and policies.

routing protocol A routing protocol is used to determine the correct route for packets within IP and IP/MPLS networks.

S

service-level agreement

See SLA.

SLA

service-level agreement

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

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 most 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.

SNMP trap log ID

SNMP trap log ID is the ID of a log. A valid log ID must exist for alarms and traps to be sent to the trap receiver.

Solaris

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

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 centre

TCP

transmission control protocol

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

Telnet

Telnet is the Internet-standard TCP/IP protocol for remote terminal connection service. It allows a user at one site to interact with a remote timesharing system at another site as if the user’s terminal connected directly to the remote machine.

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

tiered architecture Tiered architecture refers to the way in which the GUI and the network management components use a Java-based technology that provides distributed, secure, and scalable applications. This tiered architecture allows for scaling and fair load balancing, which improves performance.

U

UDP user datagram protocol

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

UI user interface

See GUI

V

VLL virtual leased line

W

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

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

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

Customer documentation and product support

Customer documentation

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

Product manuals and documentation updates are available through the Alcatel Support Documentation and Software Download service at Alcatel.com. If you are a new user and require access to this service, please contact your Alcatel sales representative.

Technical support

http://www.alcatel.com/support/

Customer documentation feedback

documentation.feedback@alcatel.com

ALCATEL