Alcatel-Lucent 5620

SERVICE AWARE MANAGER

TROUBLESHOOTING GUIDE

Alcatel·Lucent

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

Disclaimers

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

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

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

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

Contents

Troubleshooting overview

Troubleshooting the managed network

Network management troubleshooting

Troubleshooting overview

1 — 5620 SAM troubleshooting

1 — 5620 SAM troubleshooting

1.1 5620 SAM troubleshooting overview

The *5620 SAM Troubleshooting Guide* is intended for NOC operators and other engineering operational staff who are responsible for identifying and resolving performance issues in a 5620 SAM-managed network or on a 5620 SAM system. This guide covers the following general troubleshooting areas:

- managed-NE network troubleshooting
- network management domain troubleshooting
- 5620 SAM platform, database, server, or client troubleshooting

Troubleshooting the managed-NE network

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

Alarms for network objects

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

See chapters 2 and 4 for more information about using the 5620 SAM alarm information to troubleshoot a network.

Service problems with no associated alarms

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

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

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

See chapter 3 for more information about using the 5620 SAM service information to troubleshoot your network.

Troubleshooting the network management domain

The 5620 SAM has a number of powerful troubleshooting tools that help to quickly pinpoint the root cause of network and service management problems to speed resolution. Troubleshooting the client, server, or database component in a 5620 SAM network management domain requires familiarity with the following:

- the component OS
- the component configuration
- network connections to other components
- TCP/IP networking

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

Troubleshooting the 5620 SAM platform, database, server, or clients

Troubleshooting 5620 SAM related platform, database, server, or clients problem include the following common issues:

- platform problems such as slow processing or performance, excessive disk activity, or not enough swap space
- database issues such as corruption or failure, insufficient disk space, performance issues, or determining the status of the database
- server issues such as communication problems, slow response times, server-related alarms or statistics issues, or the server cannot manage new devices
- client GUIs and client OSS applications problems such as client startup issues, communication problems, slow response times, or client shut-down issues

1.2 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 System Administrator Guide* for more information about how to perform routine maintenance on your network.

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 1.6 for information about how the problem-solving model aligns with using the 5620 SAM to troubleshoot a 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 System Administrator Guide* for more information on how to generate baseline information for 5620 SAM applications.

Categorize the problem

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

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

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

Use the following guidelines to help you categorize the problem:

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

Identify the root cause of the problem

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

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

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

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

Plan corrective action and resolve the problem

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

1 Document each step of the corrective action.

2 Test the corrective action.

3 Use the CLI to verify behavior changes in each step.

4 Apply the corrective action to the live network.

5 Test to verify that the corrective action resolved the problem.

Verify the solution to the problem

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

1.3 Troubleshooting guidelines

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

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

During troubleshooting:

- Keep both the Alcatel-Lucent documentation and your company policies and procedures nearby.
- Check the appropriate release notice from the Support Documentation Service at http://support.alcatel-lucent.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 1-2 to collect the appropriate information before you call support.
- Contact your TAC or technical support representative if your company guidelines conflict with Alcatel-Lucent documentation recommendations or procedures.
- Perform troubleshooting based on your network requirements.

1.4 5620 SAM troubleshooting tools

The 5620 SAM supports a number of troubleshooting 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 for network troubleshooting and for verifying compliance with SLAs. See "STM OAM diagnostics for troubleshooting" in section 3.1 for more information.

Ethernet CFM diagnostics

Ethernet CFM diagnostic tests detect connectivity failures between pairs of local and remote maintenance end points, or MEPs, in a MEG. Each MEP is a reference point that can initiate or terminate one of the following diagnostic tests:

- CFM continuity check
- CFM loopback
- CFM link trace
- CFM Eth test
- CFM two-way delay
- CFM one-way delay
- CFM single-ended loss (7705 SAR only)
- CFM two-way SLM

See the *5620 SAM User Guide* for more information about Ethernet CFM diagnostic.

RCA audit tool

The 5620 SAM RCA audit tool allows you to perform on-demand or scheduled verifications of the configuration of services and physical links to identify possible configuration problems. Except for physical links, the 5620 SAM provides a solution, which, at your request, can automatically be implemented to make all the required configuration changes.

You can perform RCA audits of the following objects:

- VLL services
- VPLSs
- VPRN services
- physical links
- OSPF interfaces, areas, and area sites (5620 SAM/5650 CPAM integration only)
- IS-IS interfaces and sites (5620 SAM/5650 CPAM integration only)

See the *5620 SAM User Guide* for more information about the RCA audit tool.

5620 SAM log files

You can use 5620 SAM log files to help troubleshoot your network. The log files can consume a large amount of disk space during a long period of significant activity. Ensure that the contents of the various log directories are backed up on a regular basis. See the *5620 SAM System Administrator Guide* for more information about how to perform routine 5620 SAM system maintenance. See Procedure 10-1 for information about collecting 5620 SAM log files.

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

5620 SAM LogViewer

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

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

See Chapter 11 for more information about the 5620 SAM LogViewer.

User activity log

The 5620 SAM database records each 5620 SAM GUI and OSS ouser action. The 5620 SAM User Activity form allows an operator with the appropriate privilege level to list and view the 5620 SAM GUI and OSS client user activity, and to navigate directly to the object of a user action. You can also open a pre-filtered list of the recent activity for an object from the object properties form.

See the *5620 SAM User Guide* for detailed information about the user activity log. See Chapter 9 for information about using the user activity log for troubleshooting.

1.5 Before you call support

Collect the information listed in Table 1-1 before you contact Alcatel-Lucent technical support. The list of Alcatel-Lucent support contacts is available at the following URL:

http://support.alcatel-lucent.com.

Table 1-1 Required technical-support Information

Information type	Description
Issue description	• recent 5620 SAM GUI or OSS operations • screen captures or text versions of error or information messages • actions performed in response to the issue

Platform and software specifications	• 5620 SAM software release ID
	• OS type, release, and patch level
	• hardware information such as the following:
	  • CPU type
	  • number of CPUs
	  • disk sizes, partition layouts, and RAID configuration
	  • amount of RAM

System and application logs	You can run the following script on a server station to collect the required log files for Alcatel-Lucent technical support: *install_directory*/nms/bin/getDebugFiles.bash See chapter 10 for information about using the script.

1.6 Workflow to troubleshoot a problem in the 5620 SAM

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

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

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

Table 1-2 5620 SAM general troubleshooting type descriptions

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

(1 of 2)

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

(2 of 2)

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

a Use Table 1-3 to identify the appropriate 5620 SAM Managed NE network troubleshooting procedure for the problem.

b Use Table 1-4 to identify the appropriate 5620 SAM Network management domain troubleshooting procedure for the problem.

c Use Table 1-5 to identify the appropriate 5620 SAM platform, database, server, or client troubleshooting procedure for the problem.

Table 1-3 5620 SAM Managed NE network problems or tasks

Problem or tasks	Solution
Troubleshooting with alarms	
To view and sort alarms in the dynamic alarm list	Procedure 2-1
To view object alarms and aggregated object alarms	Procedure 2-2
To categorize alarms by object hierarchy	Procedure 2-3
To acknowledge alarms	Procedure 2-4
To determine probable cause and root cause using alarm and affected object information	Procedure 2-5
To determine root cause using related objects	Procedure 2-6
To troubleshoot a service equipment problem	Procedure 2-7
To clear alarms related to an equipment problem	Procedure 2-8
To troubleshoot an underlying port state problem	Procedure 2-9
To clear alarms related to an underlying port state problem	Procedure 2-10
To troubleshoot a service configuration problem	Procedure 2-11
To clear a Frame Size Problem (MTU Mismatch) alarm	Procedure 2-12
Troubleshooting services and connectivity	
To identify whether a VPLS is part of an H-VPLS	Procedure 3-1
To verify the operational and administrative states of service components	Procedure 3-2
To verify the FIB configuration	Procedure 3-3

(1 of 2)

Problem or tasks	Solution
To verify connectivity for all egress points in a service using MAC Ping and MAC Trace	Procedure 3-4
To verify connectivity for all egress points in a service using MEF MAC Ping	Procedure 3-5
To measure frame transmission size on a service using MTU Ping	Procedure 3-6
To verify the end-to-end connectivity of a service using Service Site Ping	Procedure 3-7
To verify the end-to-end connectivity of a service tunnel using Tunnel Ping	Procedure 3-8
To verify end-to-end connectivity of an MPLS LSP using LSP Ping	Procedure 3-9
To review the route for an MPLS LSP using LSP Trace	Procedure 3-10
To review ACL filter properties	Procedure 3-11
To view anti-spoof filters	Procedure 3-12
To retrieve MIB information from a GNE using the snmpDump utility	Procedure 3-13
Troubleshooting using topology maps	
To monitor alarm status on maps	Procedure 4-1
To find the source of an alarm using a map	Procedure 4-2

(2 of 2)

Table 1-4 5620 SAM Network management domain problems or tasks

Problem or task	Solution
Troubleshooting network management LAN issues	
Problem: All network management domain stations experience performance degradation	Procedure 6-1
Problem: Lost connectivity to one or more network management domain stations	Procedure 6-2
Problem: Another station can be pinged, but some functions are unavailable	Procedure 6-3
Problem: Packet size and fragmentation issues	Procedure 6-4
Troubleshooting using 5620 SAM client GUI warning messages	
Troubleshooting using 5620 SAM client GUI warning messages	Procedure 7-1
Troubleshooting with Problem Encountered forms	
To view additional problem information	Procedure 8-1
To collect problem information for technical support	Procedure 8-2
Troubleshooting with the client activity log	
To identify the user activity for a network object	Procedure 9-1
To identify the user activity for a 5620 SAM object	Procedure 9-2
To navigate to the object of a user action	Procedure 9-3
To view the user activity records of an object	Procedure 9-4

Table 1-5 5620 SAM platform, database, server, or client problems or tasks

Problem or task	Solution
Troubleshooting 5620 SAM platform problems	
To collect the 5620 SAM log files	Procedure 10-1
Problem: Poor performance on a RHEL or Solaris station	Procedure 10-2
Problem: Device discovery fails because of exceeded RHEL ARP cache	Procedure 10-3
Troubleshooting with the 5620 SAM LogViewer	
To display logs using the LogViewer GUI	Procedure 11-1
To configure the LogViewer application using the GUI	Procedure 11-2
To show or hide buttons from the LogViewer main tool bar	Procedure 11-4
To set highlight colors and fonts for LogViewer components and levels	Procedure 11-5
To automatically show or hide log messages	Procedure 11-6
To manage filters using the GUI Filter Manager	Procedure 11-7
To specify a plug-in using the LogViewer GUI	Procedure 11-8
To display logs using the LogViewer CLI	Procedure 11-9
To configure the LogViewer CLI	Procedure 11-10
To specify plug-ins using the CLI	Procedure 11-11

(1 of 3)

Problem or task	Solution
Troubleshooting the 5620 SAM database	
Problem: Database corruption or failure	Procedure 12-1
Problem: The database is running out of disk space	Procedure 12-2
Problem: A short database backup interval is creating database performance issues	Procedure 12-3
Problem: A database restore fails and generates a No backup sets error	Procedure 12-4
Problem: Database redundancy failure	Procedure 12-5
Problem: Primary or standby database is down	Procedure 12-6
Problem: Need to verify that Oracle database and listener services are started	Procedure 12-7
Problem: Need to determine status or version of database or Oracle proxy	Procedure 12-8
Troubleshooting 5620 SAM server issues	
Problem: Cannot start a 5620 SAM server, or unsure of 5620 SAM server status	Procedure 13-1
Problem: 5620 SAM server and database not communicating	Procedure 13-2
Problem: A 5620 SAM server starts up, and then quickly shuts down	Procedure 13-3
Problem: Client not receiving server heartbeat messages	Procedure 13-4
Problem: A 5620 SAM server cannot be reached over a network	Procedure 13-5
Problem: Excessive 5620 SAM server-to-client response time	Procedure 13-6
Problem: Unable to receive alarms on the 5620 SAM, or alarm performance is degraded	Procedure 13-7
Problem: All SNMP traps from managed devices are arriving at one 5620 SAM server, or no SNMP traps are arriving	Procedure 13-8
Problem: Cannot manage new devices	Procedure 13-9
Problem: Cannot discover more than one device, or device resynchronization fails	Procedure 13-10
Problem: Slow or failed resynchronization with network devices	Procedure 13-11
Problem: Statistics are rolling over too quickly	Procedure 13-12
Problem: Unable to receive alarms on the 5620 NM from the 5620 SAM	Procedure 13-13
Troubleshooting 5620 SAM client GUIs and client OSS applications	
Problem: Cannot start 5620 SAM client, or error message during client startup	Procedure 14-1
Problem: 5620 SAM client unable to communicate with 5620 SAM server	Procedure 14-2
Problem: Delayed server response to client activity	Procedure 14-3
Problem: Cannot view 5620 SAM alarms using 5620 NM client	Procedure 14-4
Problem: Unable to print from RHEL or Solaris client	Procedure 14-5
Problem: Cannot place newly discovered device in managed state	Procedure 14-6
Problem: I performed an action, such as saving a configuration, but I cannot see any results	Procedure 14-7
Problem: Device configuration backup not occurring	Procedure 14-8
Problem: 5620 SAM client GUI shuts down regularly	Procedure 14-9
Problem: Configuration change not displayed on 5620 SAM client GUI	Procedure 14-10
Problem: List or search function takes too long to complete	Procedure 14-11
Problem: Cannot select certain menu options or cannot save certain configurations	Procedure 14-12

(2 of 3)

Problem or task	Solution
Problem: Cannot clear alarms using 5620 SAM client GUI	Procedure 14-13
Problem: The 5620 SAM client GUI does not display NE user accounts created, modified, or deleted using the CLI	Procedure 14-14

(3 of 3)

4 Verify the solution.

Troubleshooting the managed network

2 — Troubleshooting using network alarms

2.1 Troubleshooting using network alarms

Incoming alarms from network objects are displayed in the dynamic alarm list and are associated with the affected objects. When the failure of an object affects a higher-level object, an alarm called a correlated alarm is raised against the higher-level object. The original alarm is called the correlating alarm. When a correlating alarm clears, the correlated alarms clear automatically.

An alarm can be raised in response to one or more network problems. To identify the root cause of a problem, you must 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.

See the *5620 SAM Alarm Reference* for information about a specific alarm. See the *5620 SAM User Guide* for information about 5620 SAM alarm management using the Alarm Info and Alarm History forms.

2.2 Workflow to troubleshoot using network alarms

1. View and monitor alarms using the dynamic alarm list or the navigation tree:
   - **a** Use the dynamic alarm list to monitor alarms and sort them according to time received. See Procedure 2-1 for more information.
   - **b** Use the navigation tree to view object alarms and navigate to affected objects. See Procedure 2-2 for more information.
2. Categorize alarms by object hierarchy and identify the alarm that is lowest in the network object hierarchy. See Procedure 2-3 for more information.
3. Acknowledge alarms on the affected object and on the related problems. See Procedure 2-4 for more information.
4. View detailed information about the alarm to determine the probable cause or root cause of the problem. See Procedure 2-5 for more information.

   See the following sources of information:

   - dynamic alarm list and Alarm Info forms
   - managed object hierarchy table
   - alarm description tables in the *5620 SAM Alarm Reference*
5. View the affected object information to determine the probable cause or root cause of the problem. See Procedure 2-5 for more information.
6. View related object information if the root cause is not found on the affected object. See Procedure 2-6 for more information.
7. In the event of a service equipment problem which produces a series of alarms, assess the alarms in the order that they are raised. See Procedure 2-7 for more information.

8 If there is an equipment down alarm, use the equipment view of the navigation tree for more information and check the physical connections to the port. See Procedure 2-8 for more information.

9 In the event of an underlying port state problem which produces a series of alarms, assess the alarms in the order that they are raised. See Procedure 2-9 for more information.

10 As required, clear the alarms related to the underlying port state problem. See Procedure 2-10 for more information.

11 In the event of a service configuration problem which produces a series of alarms, assess the alarms in the order that they are raised. See Procedure 2-11 for more information.

12 As required, clear alarms associated with SDP binding frame size problems. See Procedure 2-12 for more information.

13 As required, use the alarm description tables, alarm statistics, and the database of historical alarms, to help interpret the data and troubleshoot network problems.

2.3 Troubleshooting using network alarms procedures

Use the following procedures to troubleshoot network problems using alarms.

Procedure 2-1 To view and sort alarms in the dynamic alarm list

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

1 In the alarm window, click on the Alarm Table tab to display the dynamic alarm list.

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

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

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

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

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

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

Consider the following:

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

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

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

3 Click on the Faults tab.

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

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

i Choose an alarm from the aggregated alarms list.

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

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

Procedure 2-3 To categorize alarms by object hierarchy

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

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

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

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

3 If you need more information about an alarm, see the *5620 SAM Alarm Reference*.

Table 2-1 Hierarchy of 5620 SAM-managed objects

Level	Managed object	Domain (class)
—	General network management or 5620 SAM objects	Accounting (accounting)
		Alarm mapping (trapmapper)
		Anti-spoofing (antispoof)
		Application assurance (isa)
		APS (aps)
		Auto-config (autoconfig)
		Database (db)
		DHCP (dhcp)
		File policy (file)
		Generic object (generic)
		LI (mirrorli)
		Mediation (mediation)
		MLD (mld)
		MSDP (msdp)
		NE security (sitesec)
		Policy (policy)
		PPP (ppp)
		RADIUS accounting (radiusaccounting)
		Residential subscriber (ressubscr)
		Schedule (schedule)
		Scheduler (vs)
		Security (security)
		Server (server)
		SNMP (snmp)
		Software (sw)
		Subscriber identification (subscrident)
		Template (template)
		VRRP (vrrp)

(1 of 3)

Level	Managed object	Domain (class)
1	Network	CAC (cac)
		CCAG (ccag)
		Circuit emulation (circem)
		IGH (igh)
		IPsec (ipsec)
		L2 (layer2)
		L2 forwarding (l2fwd)
		L3 forwarding (l3fwd)
		LAG (lag)
		Network (netw)
		NE (rtr)
		Multichassis (multichassis)
		SRRP (srrp)
2	Service	Aggregation scheduler (svq)
		Epipe (epipe)
		Ipipe (ipipe)
		NAT (nat)
		Resiliency (resiliency)
		Service management (service)
		Service mirror (mirror)
		STM (sas)
		VLANs (vlan)
		VLL (vll)
		VPLS (vpls)
		VPRN (vprn)
3	SDP binding	Service tunnel management (tunnelmgmt)
4	Tunnel	Ethernet tunnel (ethernettunnel)
		L2TP (l2tp)
		MPLS (mpls)
		Rules (rules)
		Service tunnel (svt)
5	LSP binding	MPLS (mpls)
6	LSP	
7	Session	RSVP (rsvp)
8	LDP interface or targeted peer	LDP (ldp)

(2 of 3)

Level	Managed object	Domain (class)
9	Network interface	BGP (bgp)
		IGMP (igmp)
		IS-IS (isis)
		OSPF (ospf)
		PIM (pim)
		RIP (rip)
10	Physical equipment	Equipment (equipment)
		Ethernet equipment (ethernetequipment)
		Ethernet OAM (ethernetoam)
		GNE (genericne)
		LPS (lps)
		MPR (mpr)
		RMON (rmon)
		Wireless (radioequipment)
11	SONET / SDH bundle	Bundle (bundle)
	SONET	SONET (sonet)
	SONET port/channel	SONET equipment (sonetequipment)
12	DS1 / E1 channel	TDM equipment (tdmequipment)

(3 of 3)

Procedure 2-4 To acknowledge alarms

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

1 To acknowledge the selected alarm

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

If required, add text in the Acknowledgement Text box.

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

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

2 To acknowledge multiple, correlated alarms

i Right-click on the selected alarm in the dynamic alarm list and choose Show Affected Object from the contextual menu. The properties form for the object opens.

ii Click on the Faults tab, then click on the Object Alarms, Alarms on Related Objects, or Affected Objects tab to display the alarms related to the affected object.

iii Choose all the alarms listed.

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

v Click on the OK button. A dialog box 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 2-5 To determine probable cause and root cause using alarm and affected object information

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

1 Double-click on the selected alarm in the dynamic alarm list. The Alarm Info form opens.

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

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

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

- The affected object is the root cause of the problem. The alarm probable cause is the root cause. See the *5620 SAM Alarm Reference* 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 2.4 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 2-6 to review related object information.

b If the Administrative State is Up and the Operational State is not Up or Down but states a specific problem such as Not Ready or MTU Mismatch, this is the root cause of the alarm. Correct the specified problem and all correlated alarms should clear. See section 2.4 for a sample configuration problem. If alarms still exist, perform Procedure 2-6.

c If the object Administrative State is Down, it is not the root cause of the alarm on the object; however, it may cause alarms higher in the network object hierarchy. Change the Administrative State to Up. See section 2.4 for a sample underlying port state problem. This does not clear the alarm on the affected object that you are investigating. Perform Procedure 2-6 to review related object information.

Procedure 2-6 To determine root cause using related objects

1 From the Alarm Info form for the affected object (see Procedure 2-5), click on the Affected Objects tab.

Double-click an object to open the form for that object. Click on the Faults tab, then click on the Alarms on Related Objects or Affected Objects tab. This information shows aggregated or propagated alarm information. This information is not useful for root cause analysis but is helpful in identifying other affected objects.

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

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

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

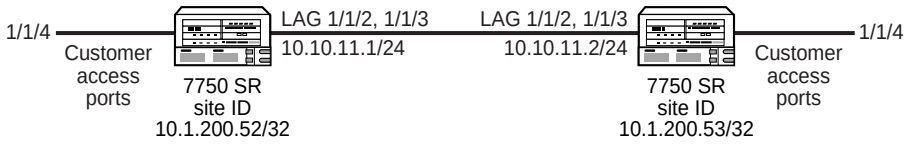
If required, check the Administrative State of the supporting port objects. A port with Administrative State Down does not generate alarms on the port, card, shelf, LAG, protocols, or sessions, but generates network path and service alarms. If the Administrative State is Down, change it to Up.

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

2.4 Sample problems

Figure 2-1 shows a two-NE 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 2-1 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 service equipment problem

An equipment problem in the sample network in Figure 2-1 produces a series of alarms. The following procedure provides an example of how to troubleshoot the problem.

Procedure 2-7 To troubleshoot a service equipment problem

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

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

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

4 Scroll through the dynamic alarm list and find the object type that is lowest in the network object hierarchy, as listed in Table 2-1.

In the sample network in Figure 2-1, 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 the sample network in Figure 2-1, 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 the sample network in Figure 2-1,

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

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

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

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

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

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

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

Procedure 2-8 To clear alarms related to an equipment problem

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

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

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

Troubleshooting an underlying port state problem

An underlying port state problem in the sample network in Figure 2-1 produces a series of alarms. The following procedure provides an example of how to troubleshoot the problem.

Procedure 2-9 To troubleshoot an underlying port state problem

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

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

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

3 Scroll through the dynamic alarm list and find the object type that is lowest in the network object hierarchy, as listed in Table 2-1.

In the sample network in Figure 2-1, the lowest-level object type in the alarm list is Lsp Path in the Path/Routing Management domain. There are two Lsp Path Down alarms. One was raised later than the other.

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

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

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

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

7 Review the information about the alarm.

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

8 Click on the View Alarmed Object button.

9 Click on the Properties button.

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

In the sample network in Figure 2-1, the Administrative State is Up and the Operational State is Down, which results in an alarm. The Operational State cannot be modified manually.

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

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

13 Find the object type that is lowest in the network object hierarchy, as listed in Table 2-1. The lowest level object is a LAG.

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

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

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

ii Click on the Port tab to view the underlying port state of the LAG member. The LAG Member 1/1/2 properties form shows the Underlying Port State: Shut Down.

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

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

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 2-10 to clear alarms related to an underlying port state problems.

Procedure 2-10 To clear alarms related to an underlying port state problem

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

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

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

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

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

5 Repeat Steps 3 and 4 for the remaining alarm.

Troubleshooting a service configuration problem

A service configuration problem in the sample network in Figure 2-1 produces a series of alarms. The following procedure provides an example of how to troubleshoot the problem.

Procedure 2-11 To troubleshoot a service configuration problem

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

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

3 Choose one of the two SDP binding alarms and acknowledge the alarm. In the sample network in Figure 2-1, the selected alarm is the SDP binding alarm raised against Site ID 10.1.200.53.

4 Select the alarms related to this affected object and acknowledge those alarms as described in Procedure 2-4.

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

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

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

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

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

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

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

8 See the *5620 SAM Alarm Reference* for additional information about the Frame Size Problem alarm.

Perform procedure 2-12 to clear the Frame Size Problem alarm.

Procedure 2-12 To clear a Frame Size Problem (MTU Mismatch) alarm

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

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

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

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

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

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

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

7 Click on the Properties button. The Site form opens with the General tab displayed.

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

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

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

11 Click the Apply button. The warning message described previously appears again.

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

3 — Troubleshooting services and connectivity

3.1 Troubleshooting services and connectivity

This chapter documents how to troubleshoot service and general connectivity problems when there is no associated alarm condition. See chapter 2 for information about troubleshooting a service using 5620 SAM alarms.

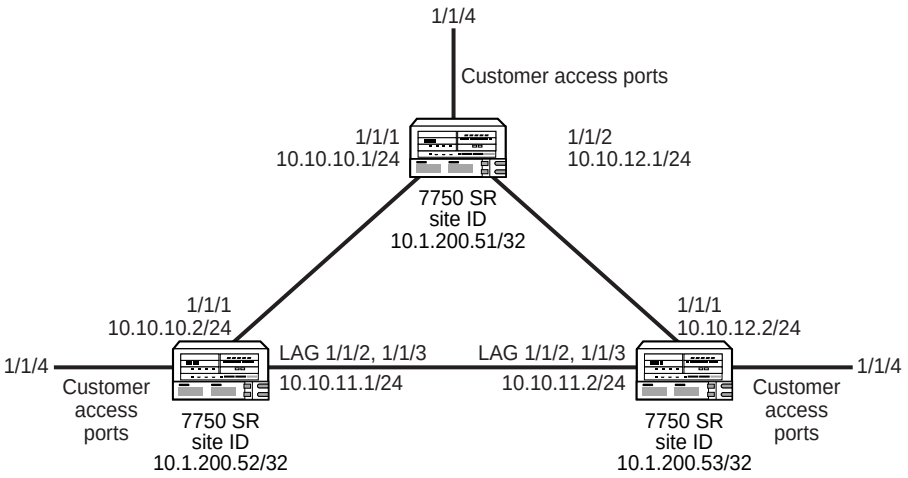
STM OAM diagnostics for troubleshooting

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

Sample network

Figure 3-1 shows a network that is used as an example for the OAM diagnostics procedures in this chapter.

Figure 3-1 Sample network



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

17557

3.2 Workflow to troubleshoot a service or connectivity problem

Perform the following tasks in sequence until you identify the root cause of the problem.

1. Verify that there are no alarms associated with the service by clicking on the Faults tab in the Service form.
   - **a** If there are alarms that affect the service, see chapter 2 for more information.
   - **b** If there are no alarms that affect the service, go to step 2 for more information.
2. If you are troubleshooting a VPLS service, determine whether it is part of an H-VPLS configuration. See Procedure 3-1 for more information.
3. Verify whether the administrative and operational states of each component of the service are Up. See Procedure 3-2 for more information.
4. Verify the connectivity of the customer equipment using the entries in the FIB. See Procedure 3-3 for more information.
5. 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.
6. Verify the connectivity of all egress points in the service:
   - **a** using MAC Ping and MAC Trace. See Procedure 3-4 for more information.
   - **b** using MEF MAC Ping. See Procedure 3-5 for more information.
7. Use the results from the MAC Ping and MAC Trace diagnostics to choose one of the following options:
   - **a** If the MAC Ping, MEF MAC Ping, or MAC Trace diagnostics returned the expected results for the configuration of your network:
     - **i** Measure the frame transmission size on all objects associated with the service such as the service sites, access and network ports, service tunnels, and circuits. See Procedure 3-6 for more information.
     - **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 3-11 for more information.
     - **iii** Verify the QoS configuration.

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

i Verify the end-to-end connectivity on the service using the Service Site Ping diagnostic. See Procedure 3-7 for more information.

ii Verify the end-to-end connectivity on the service tunnel using the Tunnel Ping diagnostic. See Procedure 3-8 for more information.

iii Verify the end-to-end connectivity of an MPLS LSP using the LSP Ping diagnostic. See Procedure 3-9 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 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 3-10 for more information.

8 As required, perform one or more of the following.

a Review ACL filter properties. See Procedure 3-11 for more information.

b View anti-spoof filters. See Procedure 3-12 for more information.

c Retrieve MIB information from a GNE using the snmpDump utility. See Procedure 3-13 for more information.

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

3.3 Service and connectivity troubleshooting procedures

Use the following procedures to perform service and connectivity troubleshooting.

Procedure 3-1 To identify whether a VPLS is part of an H-VPLS

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

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

3 Choose the service associated with the service problem.

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

5 Click on the Mesh SDP Bindings or Spoke SDP Bindings tab.

6 Drag and drop the Service ID, VC ID, and Service Type columns to first three positions on the left side of the form.

7 Sort the list by VC ID.

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

a If there are no alarms on the H-VPLS service, go to step 3 in section 3.2.

b If there are alarms on the H-VPLS service, see chapter 2 for more information.

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

Procedure 3-2 To verify the operational and administrative states of service components

1 Open the service properties form.

2 On the navigation tree, click on the site on which you want to verify the operational and administrative states of service components; expand the entries for that site.

3 Click on the site. The *service* (Edit) form opens with the General tab displayed. Review the states for the site using the Operational State and Administrative State parameters.

4 On the navigation tree, click on the L2 Access Interfaces, L3 Access Interfaces, and Mesh SDP Bindings or Spoke SDP bindings objects to review the operational and administrative states for the remaining components of the service.

5 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 4 in section 3.2.

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 2 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 7.

6 If the service problem persists, another type of service problem may be present. Perform the steps of the section 3.2 troubleshooting workflow.

7 If the workflow does not identify the problem with your service, contact your Alcatel-Lucent technical support representative. See chapter 1 for more information.

Procedure 3-3 To verify the FIB configuration

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

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

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

3 Click on the Forwarding Control tab.

4 Click on the FIB Entries tab.

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 5 in section 3.2.
- **b** If there are no FIB entries, there is a configuration problem with the customer equipment or the connection from the equipment to the service tunnel.
  - **i** Confirm that the 5620 SAM service configuration aligns with the customer requirements.
  - **ii** Confirm that there are no problems with the customer equipment and associated configuration.

6 If the service problem persists, another type of service problem may be present. Perform the steps of the section 3.2 troubleshooting workflow.

7 If the workflow does not identify the problem with your service, contact your Alcatel-Lucent technical support representative. See chapter 1 for more information.

Procedure 3-4 To verify connectivity for all egress points in a service using MAC Ping and MAC Trace

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

2 Click on the Create button.

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

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

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

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

a You can target the MAC broadcast address of FF-FF-FF-FF-FF-FF in the data plane to flood the service domain and receive a response from all operational service access ports. Enter the service ID for the VPLS or VLL service between the sites, and the sites you want to ping, in this case, from site ID 10.1.200.51/32 to site IDs 10.1.200.52/32 and 10.1.200.53/32 using the network in Figure 3-1.

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

b You can target the specific MAC address of a service site. Enter the target MAC address of the specific site in the service that you want to ping, in this case, from site ID 10.1.200.51/32 to site ID 10.1.200.52/32 using the network in Figure 3-1.

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

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

In particular, review the results in the Return Code column. Table 3-1 lists the displayed messages.

Table 3-1 MAC Ping OAM diagnostic results

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

(1 of 2)

Displayed message	Description
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.

(2 of 2)

7 Click on the Create button.

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

9 Configure the parameters for the diagnostic session and run the diagnostic. A MAC Trace shows the path, protocol, label, destination SAP, and hop count to the location of the destination MAC. Enter the service ID for the VPLS or VLL service between the sites, and the sites you want to trace, in this case, from site ID 10.1.200.51/32 to site IDs 10.1.200.52/32 and 10.1.200.53/32 using the network in Figure 3-1.

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

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

a If MAC Ping and MAC Trace diagnostics returned the expected results for the configuration of your network, go to step 7 a in section 3.2.

b If MAC Ping and MAC Trace diagnostics did not return the expected results for the configuration of your network, go to step 7 b in section 3.2.

c Go to step 7 c in section 3.2 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 3-5 To verify connectivity for all egress points in a service using MEF MAC Ping

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

2 Click on the Create button.

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

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

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

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

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

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

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

In particular, review the results in the Return Code column. Table 3-2 lists the displayed messages.

Table 3-2 MEF MAC Ping OAM diagnostic results

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

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

a If MEF MAC Ping diagnostics returned the expected results for the configuration of your network, go to step 7 a in section 3.2.

Procedure 3-6 To measure frame transmission size on a service using MTU Ping

1 Record the maximum frame transmission size for the service.

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

3 Filter to list only the source and destination routers of the service tunnel and click on the Search button. The list of service tunnels appears.

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

5 Click on the Tests tab.

6 Click on the MTU Ping tab.

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

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

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

9 Run the diagnostic. The MTU Ping increments the datagram size until it fails to pass through the SDP (service tunnel) data path, in this case, an MTU Ping from site ID 10.1.200.52/32 to site ID 10.1.200.53/32 using the network in Figure 3-1.

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

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

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 7 a ii in section 3.2.

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

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

12 If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel-Lucent technical support representative. See chapter 1 for more information.

Procedure 3-7 To verify the end-to-end connectivity of a service using Service Site Ping

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

2 Click on the Create button.

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

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

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

The originating service tunnel for the Service Site Ping is from site ID 10.1.200.51/32 to site ID 10.1.200.53/32, the other end of the service using the network in Figure 3-1.

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

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

Table 3-3 lists the displayed messages.

Table 3-3 Service Site Ping OAM diagnostic results

Displayed message	Description
Sent - Request Timeout	The request timed out with a reply.
Sent - Request Terminated	The request was not sent because the diagnostic was terminated by the operator.
Sent - Reply Received	The request was sent and a successful reply message was received.
Not Sent - Non-Existent Service-ID	The configured service ID does not exist.
Not Sent - Non-Existent SDP for Service	There is no SDP for the service tested.
Not Sent - SDP For Service Down	The SDP for the service is down.
Not Sent - Non-Existent Service Egress Label	There is a service label mismatch between the originator and the responder.

a If the Service Site ping passes, the routes between the two sites are complete and in an operational state. If the MAC Ping performed in Procedure 3-4 failed:

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

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

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

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

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

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

ii Enter the following command:

`ping <destination_site_ip_address>` ↵

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

If the CLI IP ping passes, go to step 7 b ii of the section 3.2 troubleshooting workflow.

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

`show router route-table` ↵

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

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

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

7 If the service problem persists, another type of service problem may be present. Perform the steps of the section 3.2 troubleshooting workflow.

8 If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel-Lucent technical support representative. See chapter 1 for more information.

Procedure 3-8 To verify the end-to-end connectivity of a service tunnel using Tunnel Ping

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

2 Filter to list only the source and destination routers of the service tunnel and click on the Search button. The list of service tunnels appears.

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

4 Click on the Tests tab.

5 Click on the Tunnel Ping tab.

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

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

7 Configure the parameters for the diagnostic session as follows.

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

8 Run the diagnostic. Set the diagnostic configuration for a Tunnel Ping from site ID 10.1.200.51/32 to site ID 10.1.200.53/32 using the network in Figure 3-1, by specifying the return ID of the tunnel you want to test.

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

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

Table 3-4 lists the displayed messages.

Table 3-4 Tunnel OAM diagnostic results

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

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

b If the Tunnel Ping fails, go to step 7 b iii of the section 3.2 troubleshooting workflow to verify the end-to-end connectivity of services using MPLS LSP paths, if required.

10 If the service problem persists, another type of service problem may be present. Perform the steps of the section 3.2 troubleshooting workflow.

11 If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel-Lucent technical support representative. See chapter 1 for more information.

Procedure 3-9 To verify end-to-end connectivity of an MPLS LSP using LSP Ping

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

2 Click on the Create button.

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

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

4 Configure the parameters for the diagnostic session and run the diagnostic. Target an LSP or an LSP path. Choose the MPLS site for the test, then configure the LSP you want to ping that is associated with the MPLS site, in this case, an LSP Ping from site ID 10.1.200.51/32 to site ID 10.1.200.52/32 using the network in Figure 3-1.

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

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

Table 3-5 lists the displayed messages.

Table 3-5 LSP Ping OAM diagnostic results

Displayed message	Description
notApplicable (0)	The OAM diagnostic message does not apply to the OAM diagnostic performed.
fecEgress (1)	The replying router is an egress for the FEC. The far-end egress point exists and is operating correctly. No action required.
fecNoMap (2)	The replying router has no mapping for the FEC.
notDownstream (3)	The replying router is not a downstream router.
downstream (4)	The replying router is a downstream router, and the mapping for this FEC on the router interface is the specified label.
downstreamNotLabel (5)	The replying router is a downstream router, and the mapping for this FEC on the router interface is not the specified label.
downstreamNotMac (6)	The replying router is a downstream router, but it does not have the specified MAC address.
downstreamNotMacFlood (7)	The replying router is a downstream router, but it does not have the specified MAC address and cannot flood the request to other routers.
malformedEchoRequest (8)	The received echo request is malformed.
tlvNotUnderstood (9)	One or more TLVs were not understood.

a If the LSP Ping passes, you have completed the workflow for troubleshooting services. Contact your Alcatel-Lucent technical support representative if the problem persists. See chapter 1 for more information.

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

6 If the service problem persists, another type of service problem may be present. Perform the steps of the section 3.2 troubleshooting workflow.

7 If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel-Lucent technical support representative. See chapter 1 for more information.

Procedure 3-10 To review the route for an MPLS LSP using LSP Trace

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

2 Click on the Create button.

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

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

4 Configure the parameters for the diagnostic session and run the diagnostic. Target an LSP, any LSP or an LSP path. Choose the MPLS site for the test, then configure the LSP or LDP you want to trace that is associated with the MPLS site, in this case, an LSP Ping from site ID 10.1.200.51/32 to site ID 10.1.200.52/32 using the network in Figure 3-1.

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

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

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

6 If the service problem persists, another type of service problem may be present. Perform the steps of the section 3.2 troubleshooting workflow.

7 If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel-Lucent technical support representative. See chapter 1 for more information.

Procedure 3-11 To review ACL filter properties

1 Click on the L2 Access Interfaces or L3 Access Interfaces tabs on the Services (Edit) form. A list of interfaces appears.

2 Double-click on a row in the list. The L2 or L3 Interface configuration form appears.

3 Click on the ACL tab.

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 7 a ii in section 3.2.
- **b** If there are ACL filtering configurations that interfere with the service traffic, implement and verify the solution for the service problem.

5 If the service problem persists, another type of service problem may be present. Perform the steps of the section 3.2 troubleshooting workflow.

6 If the troubleshooting workflow does not identify the problem with your service, contact your Alcatel-Lucent technical support representative. See chapter 1 for more information.

Procedure 3-12 To view anti-spoof filters

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

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

1 Select Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

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

3 Select the service in the list for which you want to view the anti-spoof filters.

4 Click on the Properties button. The Service (Edit) form opens with the General tab displayed.

5 Click on the L2 Access Interfaces or L3 Access Interfaces tab, depending on the service that you selected.

6 Select an interface from the list and click on the Properties button. The Access Interface (Edit) form opens with the General tab displayed.

7 Click on the Anti-Spoofing tab.

8 Click on the Filters tab.

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

Procedure 3-13 To retrieve MIB information from a GNE using the snmpDump utility

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

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

2 Open a console window.

3 Navigate to the *install_dir*/nms/bin directory

where *install_dir* is the main server installation location, typically /opt/5620sam/server

4 Enter the following at the prompt:

./snmpDump.bash *option_list* ↵

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

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

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

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

Table 3-6 snmpDump .bash options

Option	Description
-v *version*	The SNMP version in use on the GNE Default: 2
-f *file_name*	The output filename Default: *host*-snmpDump.out in the current directory
-h *host*	The IP address or hostname of the GNE Default: localhost
-c *community*	The SNMP community
-u *v3_user*	The SNMPv3 user name
-e *snmp_engine_ID*	The SNMP engine ID
-ap *v3_auth_protocol*	The SNMPv3 authorization protocol, which can be MD5 or SHA Default: MD5
-apw *v3_auth_password*	The SNMPv3 authorization password
-ppw *v3_privacy_password*	The SNMPv3 privacy password
-cn *v3_context_name*	The SNMPv3 context name
-ci *v3_context_ID*	The SNMPv3 context ID

(1 of 2)

Option	Description
-p *port*	The TCP port on the main server that snmpDump must use to reach the GNE Default: 161
-t *timeout*	A communication timeout value
-r *retries*	The number of times to retry connecting to the GNE

(2 of 2)

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

```
Init Products ...

Init ProductFamilyDefs ...

Init PollingDirectiveDefs ...

Start reading from Node ...
```

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

```
IF-MIB.ifEntry : 21

IP-MIB.ipAddrEntry : 5

MPLS-LSR-STD-MIB.mplsInterfaceEntry : 8

MPLS-TE-STD-MIB.mplsTunnelEntry : 0

MPLS-TE-STD-MIB.mplsTunnelHopEntry : 0

MPLS-TE-STD-MIB.mplsTunnelARHopEntry : 0

MPLS-TE-STD-MIB.mplsTunnelCHopEntry : 0

MPLS-LDP-STD-MIB.mplsLdpEntityEntry : 3

MPLS-LDP-STD-MIB.mplsLdpEntityStatsEntry : 3

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

The utility is finished when the command prompt is displayed.

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

4 — Troubleshooting using topology maps

4.1 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*.

Table 4-1 describes the tasks associated with troubleshooting the 5620 SAM using Network topology maps.

Table 4-1 Network topology map tasks

Problem	Solution
To monitor alarm status on maps	Procedure 4-1
To find the source of an alarm using a map	Procedure 4-2

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

Table 4-2 lists the maps that are available and how they are accessed.

Table 4-2 5620 SAM map views

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

(1 of 2)

Menu option	Function
Create→Equipment→Physical Link	Create physical links to view L1 network connectivity.

(2 of 2)

The maps represent interfaces, paths, managed devices, and unmanaged devices, as described in Table 4-3.

Table 4-3 Map elements

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

Interpreting map status indicators

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

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

Table 4-4 describes the map status indicators. There are no status indicators for unmanaged devices.

Table 4-4 Map status indicators

Indicator	Description
Device icon color	The color of device icons and links represents the reachability of the device. Red indicates that the device or link is not SNMP reachable. Yellow indicates that the device is being synchronized. Green indicates that the device is SNMP reachable. For a service view, red indicates that the service on the device is down.

(1 of 2)

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

(2 of 2)

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

Table 4-5 Map alarm status indicators

Map icon		Alarm	
Icon symbol	**Icon color**	**Severity**	**Color**
—	—	All	Grey
C	Red	Critical	Red
M	Orange	Major	Orange
m	Yellow	Minor	Yellow
W	Cyan	Warning	Cyan
Cn	Mocha	Condition	Mocha
—	Green	Cleared	Green
i	Light blue	Info	Light blue
I	White	Indeterminate	White

4.2 Troubleshooting alarms using topology maps

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

Procedure 4-1 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 4-2 for information on how to access maps.

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

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

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

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

5 Perform Procedure 4-2 to troubleshoot any problems that may arise.

Procedure 4-2 To find the source of an alarm using a map

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

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

2 Right-click to view the contextual menu.

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

b When you right-click on an interface:

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

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

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

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

4 View alarm status and diagnose the problem, as described in chapter 2.

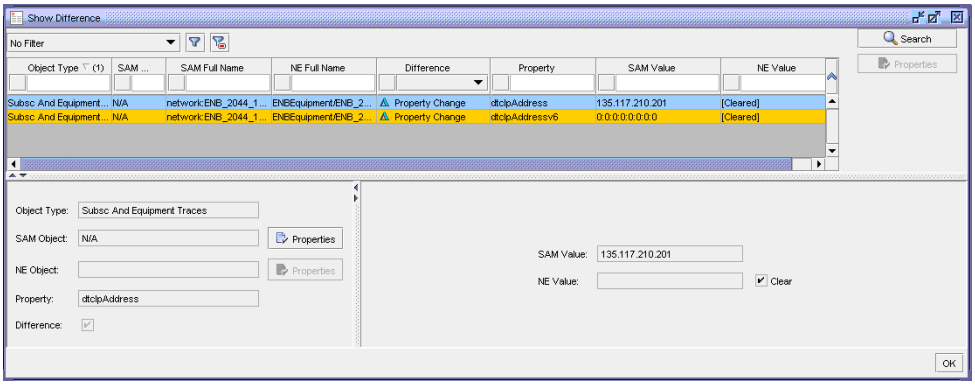
5 — Troubleshooting using the NE resync audit function

5.1 NE resync audit overview

You can use the NE resync audit function of the 5620 SAM to detect and report differences between the 5620 SAM and the NE configuration. This function is helpful for troubleshooting configuration misalignment. The NE resync audit manager displays a list of misaligned parameters and values as represented in the NE and 5620 SAM databases, and provides quick navigation to the affected object. A resync audit polls the NE in the same manner as a standard full resynchronization, but instead of updating the objects in the 5620 SAM database, the 5620 SAM compares the NE configuration retrieved by the resync with the NE configuration in the 5620 SAM. See Procedure 5-1 for information about performing an NE resync audit.

Differences identified during the audit are displayed in the Show Difference manager. In this manager, you can navigate to the associated NE object that contains the difference and perform a resync on that object to resolve the difference. You can access the results of one audit per NE in the NE audit result list. See Procedure 5-2 for information about viewing NE audit results. See Figure 5-1 for an example of the Show Difference manager displaying configuration misalignment for an NE.

Figure 5-1 Show Differences manager displaying misalignment



You can specify whether to include or ignore read-only parameters in a resync audit. Some read-only parameters are set by the NE after a configuration change. Other read-only parameters, such as temperature measurements and time stamps, change frequently on the NE and will often differ from the values in the 5620 SAM database. Disabling the inclusion of read-only parameters can help prevent cluttered audit results.

The difference entries that an NE resync audit returns are categorized as follows:

- Property Change—the value of a specific parameter is different in the 5620 SAM and NE databases
- Missing—the object and contained parameters exist in the 5620 SAM, but not on the NE
- Added—the object and contained parameters exist on the NE, but not in the 5620 SAM

Additional information

Consider the following information about NE resync audits:

- The 5620 SAM limits the audit result to 1 000 differences.
- NE resync audits only compare parameters that are synchronized with the 5620 SAM database. Parameters that are stored in the NE database only and are not managed by the 5620 SAM are not included in the audit report.
- NE resync audit results do not include statistics.
- NE resync audits cannot be used to deploy changes to an NE.
- You cannot perform a full resync from the NE audit manager or Show Differences form.

5.2 Workflow for NE resync auditing

1 Perform NE resync auditing to identify specific object and parameter misalignment between eNodeB and the 5620 SAM; see Procedure 5-1.

2 View the results of NE resync audits and manage audit results; see Procedure 5-2.

5.3 NE resync auditing procedures

Perform the following procedures to manage NE resync auditing.

Procedure 5-1 To perform an NE resync audit

1 Choose Equipment from the navigation tree view selector. The managed NEs are displayed.

2 Right-click on an NE and choose NE Resync Audit from the contextual menu. A dialog box appears.

3 Enable the check box if you want to include read-only attributes in the audit and click on the Yes button. The NE Audit Result form appears and displays the NE Audit State as “in progress”.

Note — The 5620 SAM displays an error message and does not begin the resync audit if the NE in unreachable.

4 When the audit completes, choose one of the following based on the NE Audit State:

   a If the NE Audit State displays “succeeded” and the NE Audit Result displays “misaligned”, go to step 5.

   b If the NE Audit State displays “succeeded” and the NE Audit Result displays “aligned”, then no further action is required.

   c If the NE Audit State displays “failed”, information about the failure is displayed in the Error Messages panel. Click to expand the panel.

5 Click on the Show Difference button. The Show Difference form opens with a list of difference entries displayed.

6 To resync a missing or added object, perform a full resync.

7 To resync a property change for a single object with the 5620 SAM:

   i Select a difference entry from the list. The panes at the bottom of the form display the misaligned data for the entry.

   ii Click on the Properties button for the SAM Object. The properties form of the object is displayed.

   iii Click on the Resync button. A dialog box appears.

   iv Click on the Yes button and wait for the object to resync with the 5620 SAM. The value of the misaligned parameter changes if the resync operation is successful.

8 To save the results of the resync audit to an HTML or CSV file:

   i Right-click on a column header in the differences list and choose Save to File from the contextual menu. The Save As form is displayed.

   ii Navigate to the required location on the client workstation and specify a file name.

   iii Choose a file type.

   iv Click on the Save button. The file is saved.

9 In the Show Difference form, click on the OK button. The form closes.

10 In the NE Audit Result form, click on the Close button. The form closes.

Procedure 5-2 To view NE resync audit results using the NE audit manager

You can use the NE audit manager to view the results of previous NE audits and delete audit results.

1 Choose Administration→NE Maintenance→NE Audit Results from the 5620 SAM main menu. The NE Audit Manager list form opens.

2 Configure the filter criteria, if required, and click on the Search button. A list of NE resync audit results is displayed.

3 To view an entry, select an entry from the list and click on the Show Difference button. If there are results to display, the Show Difference form opens.

4 To delete an entry:

   i Select an entry from the list and click on the Delete button. A dialog box appears.

   ii Click on the Yes button. The entry is deleted.

5 Close the NE Audit Manager list form.

Network management troubleshooting

6 — Troubleshooting network management LAN issues

6.1 Troubleshooting network management domain LAN issues

Table 6-1 describes the problems associated with troubleshooting network management domain LAN issues.

Table 6-1 5620 SAM Network management domain LAN problems

Problem	Solution
Problem: All network management domain stations experience performance degradation	Procedure 6-1
Problem: Lost connectivity to one or more network management domain stations	Procedure 6-2
Problem: Another station can be pinged, but some functions are unavailable	Procedure 6-3
Problem: Packet size and fragmentation issues	Procedure 6-4

6.2 Troubleshooting network management domain LAN issues procedures

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

Procedure 6-1 Problem: All network management domain stations experience performance degradation

1 Verify that there is sufficient bandwidth between the elements of the network management domain.

Bandwidth requirements vary depending on the type of management links set up, and the number of devices in the managed networks. For information about network planning expertise, contact your Alcatel-Lucent technical support representative.

See the *5620 SAM Planning Guide* for more information about the bandwidth requirements.

2 When you are using in-band management, ensure that the network devices used to transport the management traffic are up. Ping each of the devices to ensure the management traffic can flow along the in-band path.

In-band management uses a connection provided by a customer service, such as a VLL. The management traffic is sent in-band along with the customer payload traffic. The packets with the management data arrive at the device using one of the virtual interfaces.

Procedure 6-2 Problem: Lost connectivity to one or more network management domain stations

Perform this procedure to check the basic connectivity between stations.

1 Log in to the station.

2 Open a console window.

3 Enter one of the following to perform a ping connectivity check:

On a RHEL or Windows station:

ping *station* ↵

On a Solaris station:

ping -s *station* ↵

where *hostname_or_IP_address* is the station hostname or IP address

4 To interrupt the ping operation, press <CTRL>+C.

5 Review the output, which resembles the following when connectivity is good:

```
PING station: 56 data bytes

64 bytes from station (192.168.106.169): icmp_seq=1, time=1.0 ms

64 bytes from station (192.168.106.169): icmp_seq=2, time=0.3 ms

64 bytes from station (192.168.106.169): icmp_seq=3, time=0.2 ms

----station PING Statistics----

3 packets transmitted, 3 packets received, 0% packet loss

rtt (ms) min/avg/max = 0.2/0.7/1.0
```

If the packets arrive out of order, if some packets are dropped, or if some packets take too long to complete the round trip, LAN congestion may be a problem. Contact your IT department or check the physical LAN connectivity.

If you can ping a station, but are unable to connect to the station to perform a function, there may be a problem with access to an application on the station. See Procedure 6-3 for information about how to verify the following:

- ports that need to be open across firewalls
- routing configuration

6 If the 5620 SAM deployment includes a firewall, view the firewall log entries in the appropriate file:

- on a RHEL station—/var/logs/messages
- on a Solaris station—/var/adm/messages

Procedure 6-3 Problem: Another station can be pinged, but some functions are unavailable

Perform this procedure to determine whether port availability or routing is the cause of a management domain LAN issue.

The 5620 SAM uses TCP and UDP ports for communication between components. Some of the ports, such as the SNMP trap port, are configured during installation. Other ports are configured automatically by the 5620 SAM software.

1 Log in as the root user on a station in the network management domain.

2 Verify that the required ports are open or protected by a firewall. See the *5620 SAM Planning Guide* for a complete list of the ports that the 5620 SAM requires and the purpose of each port.

Note — If you modify the port configuration, ensure that you record the changes for future reference.

3 Perform the following steps to check the local routing configuration.

i Open a console window on a station in the management domain.

ii Use one of the following commands to determine the path to a destination:

- on a Windows station—tracert
- on a RHEL or Solaris station—traceroute

The command uses ICMP echo request messages to list the near-side interfaces that packets traverse between the source and destination stations. A near-side interface is the interface closest to the source host.

iii Use OS commands such as netstat -r and arp -a to display a list of active TCP connections, Ethernet statistics, the IP routing table, and the ports on which the station is listening.

Procedure 6-4 Problem: Packet size and fragmentation issues

Large packet sizes from the managed devices are being dropped by intermediate routers because the packets exceed the device MTU or the devices are not configured to forward fragmented packets, causing resynchronizations to fail. The 5620 SAM-managed devices are configured to send SNMP packets of up to 9216 bytes. The 5620 SAM is typically configured to accept large SNMP packets.

However, the typical L2 or L3 interface MTU on a 5620 SAM-managed device is likely configured to transmit smaller SNMP packets, usually in the 1500-byte range. This causes packet fragmentation. In order to handle these fragmented packets, intermediate devices between the 5620 SAM- managed device and 5620 SAM must be configured to handle or forward fragmented packets. When an intermediate network device, such as a router, cannot handle or forward fragmented packets, then packets may be dropped and resynchronization may fail. Consider the following.

- The network infrastructure that carries traffic between the 5620 SAM main and auxiliary servers and the managed NEs must support fragmentation and reassembly of the UDP packets for NEs that have an SNMP PDU size greater than the MTU configured for the network path between the NE and 5620 SAM. The

7210 SAS, 7450 ESS, 7705 SAR, 7710 SR, 7750 MG, 7750 SR, and 7950 XRS require an SNMP PDU size of 9216 bytes and fragmentation support in the network path between the 5620 SAM and the NE.

- Ensure that the CPM filters on managed devices are configured to accept fragmented packets, and that this filter policy is configured on each server in a redundant 5620 SAM deployment.
- Ensure that devices located between the managed devices, such as the 7750 SR, and the 5620 SAM can handle an MTU size of 9216 bytes, can fragment large SNMP packets, or can forward fragmented L2 or L3 packets.
- Verify the MTU packet sizes for all LAN devices.
- Verify that large packets can travel from the managed devices to the 5620 SAM by using CLI to ping the IP address of the 5620 SAM server, with a large packet.
- Ensure that the firewalls between the managed devices and the 5620 SAM server are configured to allow traceroute and ping packets.

1 Log in to the 7750 SR or another 5620 SAM-managed device.

2 Run the traceroute command:

> traceroute *SAM_server_IP_address* ↵

A list of hops and IP addresses appears.

3 Ping the first hop in the route from the managed device to the 5620 SAM server:

> ping *intermediate_device_IP_address* size 9216 ↵

A successful response indicates that the intermediate device supports large SNMP packets or packet fragmentation.

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

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

7 — Troubleshooting using 5620 SAM client GUI warning messages

7.1 5620 SAM client GUI warning message overview

Warning messages in the 5620 SAM client GUI provide an error recovery mechanism to inform you when:

- information has been entered incorrectly
- additional information is required
- the operation you are attempting cannot be completed
- a change to a configuration sub-form is not committed until the parent form is committed
- an operation that may result in service disruption is requested
- a configuration form for an object is open that can potentially conflict with a previously opened form

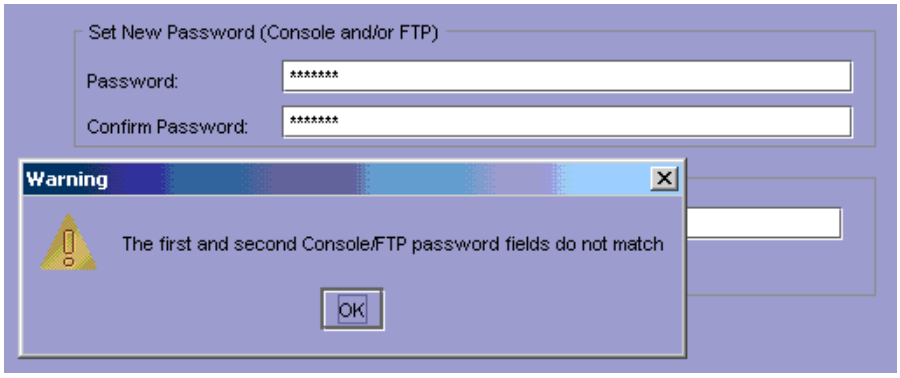
When an error condition is encountered that the 5620 SAM client has not anticipated, a Problems Encountered form is displayed. See section 8.1 for more information.

You can use the client GUI to suppress warning messages within containing windows. See the *5620 SAM User Guide* for more information.

Incorrect data entry

When incorrect information is entered for a parameter, a warning message that describes the error is displayed. For example, when you configure a password for a site user, the value entered for the Password parameter and the Confirm Password parameter must match. If they do not match, a warning message is displayed, as shown in Figure 7-1.

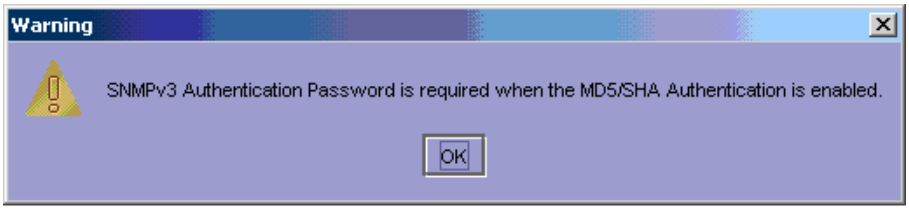
Figure 7-1 Password mismatch warning dialog box



Additional information required

When the value selected for a parameter has a that requires another parameter to be configured, a warning message indicates the missing information that is required. For example, when you configure a new or existing user with MD5 or SHA as the value for the Authentication Protocol parameter, a password must be configured. If you do not configure a password, a warning message is displayed, as shown in Figure 7-2.

Figure 7-2 Password missing warning dialog box



The warning message indicates the information that is required. In this case, click on the OK button to close the dialog box, and configure the New Authentication Password and Confirm New Auth Password parameters.

Unable to complete requested action

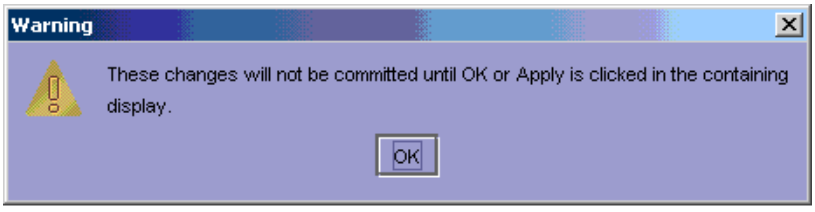
Warning messages are used to indicate that a specific action cannot be completed. These warnings may occur when you try to create a new object or modify an existing object that results in an unsupported configuration. For example, the message “Can't bind LSP to a non-mpls service tunnel“ indicates that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

These errors can be difficult to resolve and may require that you retrace your steps to determine the cause of the warning. Check the documentation to ensure that you are following procedures correctly.

Commitment of changes from a form and its sub-forms

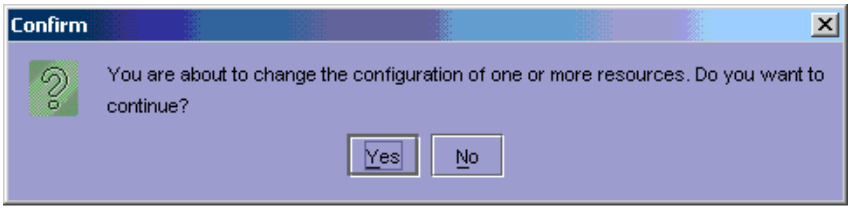
From a configuration form, you can open sub-forms that require completion before you continue with the parent form. For example, when you create a VLL service, the Create Service Site form opens during one of the configuration steps. After you configure parameters in this sub-form and click on the Finish button, a warning message is displayed, as shown in Figure 7-3.

Figure 7-3 Committing changes warning dialog box



Changes entered in the sub-form are not committed until you click on the OK or Apply button of the parent form. When you click on the OK or Apply button of the parent form, a final confirmation is displayed, as shown in Figure 7-4.

Figure 7-4 Committing changes to resources warning dialog box

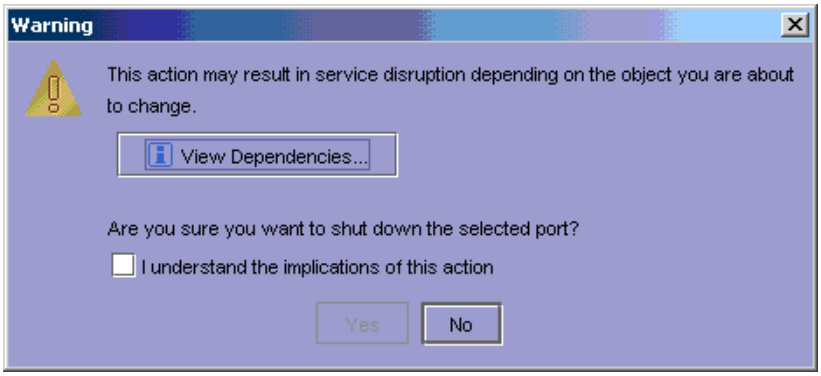


When you click on the Yes button for the last confirmation the changes to the parent or sub-forms are committed.

Service disruption warning

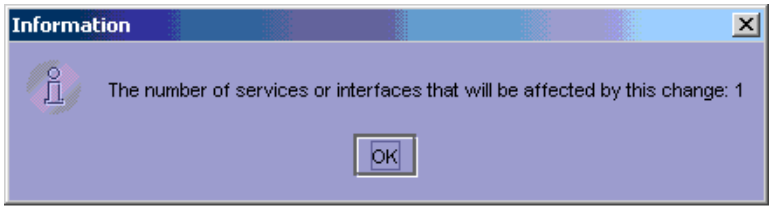
A service disruption dialog box is displayed when you perform an action that may be service-affecting. For example, if you attempt to shut down a daughter card, a warning message is displayed, as shown in Figure 7-5.

Figure 7-5 Service disruption warning dialog box



As indicated by the warning message, the action you are about to perform may cause a disruption to customer service because of a potential dependency that another object or service has on the current object. Click on the View Dependencies button to indicate the number of services that may be affected by the action, as shown in Figure 7-6.

Figure 7-6 View dependencies warning dialog box

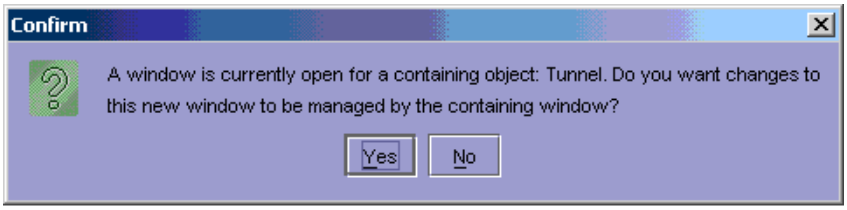


Verify that the requested action is appropriate. Click on the checkbox beside the statement “I understand the implications of this action” to continue with the action.

Duplicate configuration form conflicts

There are multiple ways to access a configuration form for the same object. For example, you can view the configuration form for a port by choosing Manage→Equipment, or you can access the port by clicking on the port object in the expanded navigation tree. When you try to perform both accesses, a warning message is displayed, as shown in Figure 7-7.

Figure 7-7 Duplicate form warning dialog box



When this warning message is displayed, another form is open for the same object. When two forms are open concurrently for the same object, there may be unexpected results because changes committed from one form are not reflected in the other form.

7.2 Responding to 5620 SAM client GUI warning messages

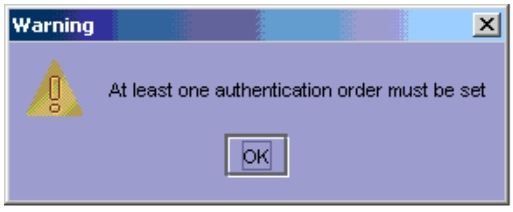
The following procedure describes how to respond to a warning message when you perform an action with the 5620 SAM client.

Procedure 7-1 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 7-8.

Figure 7-8 Authentication warning dialog box



2 After you read the warning message, click on the OK button. The warning message dialog box closes.

3 Correct the problem based on the information provided. For the example in Figure 7-8, 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, collect the logs identified in Procedure 10-1 before you contact your technical support representative.

8 — Troubleshooting with Problems Encountered forms

8.1 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 8-1 shows the Problems Encountered form.

Figure 8-1 Problems Encountered form

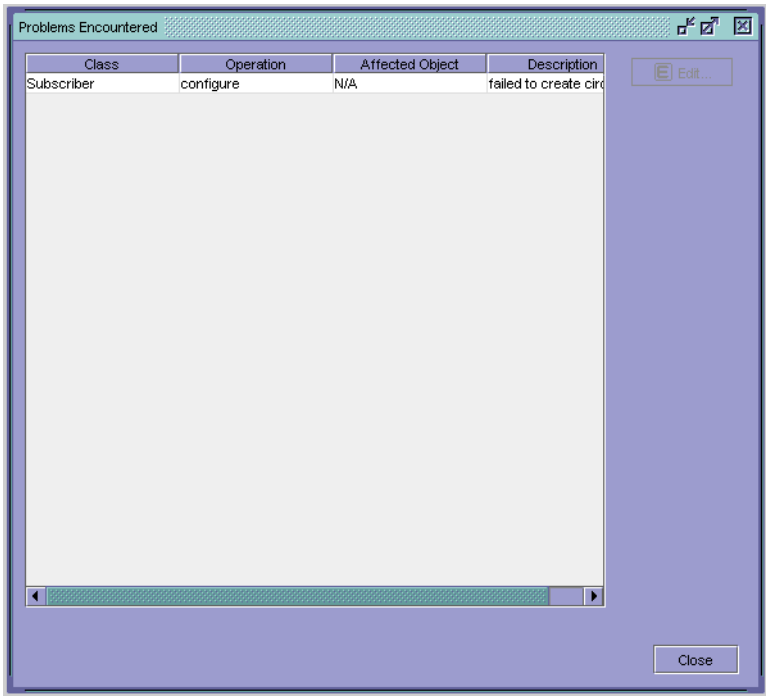


Table 8-1 describes the tasks associated with troubleshooting the 5620 SAM using the Problems Encountered form.

Table 8-1 Problems Encountered form tasks

Problem	Solution
To view additional problem information	Procedure 8-1
To collect problem information for technical support	Procedure 8-2

Table 8-2 describes the fields in the Problems Encountered form.

Table 8-2 Problems Encountered form field descriptions

Field name	Description
Class	Specifies the object type that is the source of the problem

(1 of 2)

Field name	Description
Operation	Specifies the type of operation that was attempted when the problem occurred.
Affected Object	Specifies the name of the affected object. Typically, if a Problems Encountered form appears when you are trying to create a object, this field contains N/A because the object has not been created.
Description	Specifies a short description of the problem, which may help you determine the cause of the problem and how to correct the problem. For additional information, click on the Properties button. The information may not be enough for you to correct the problem. The information can be used by your technical support representative to help resolve the problem.

(2 of 2)

8.2 Using Problems Encountered forms

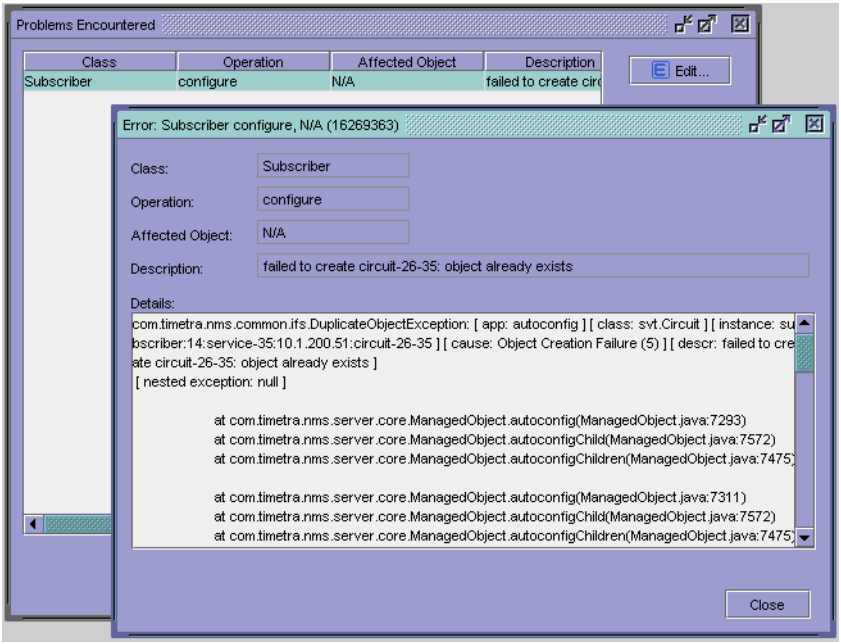
The following procedures describe how to view additional information about a problem in a Problems Encountered form and the information to collect before you contact your technical support representative.

Procedure 8-1 To view additional problem information

1 Choose an entry in the Problems Encountered form.

2 Click on the Properties button. Figure 8-2 shows a form with the problem details.

Figure 8-2 Problems Encountered form details



3 Try to correct the problem based on the information provided. If you cannot correct the problem, complete the procedure and perform Procedure 8-2.

4 Click on the Close button to close the details form.

5 If there is more than one problem, repeat steps 2 to 4.

6 Click on the Close button.

Procedure 8-2 To collect problem information for technical support

The following procedure describes what to do before you contact your technical support representative when you cannot resolve a problem on the Problems Encountered form.

1 Review the problem information in the Problems Encountered form, as described in Procedure 8-1.

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 chapter 1.

4 Collect logs for your Alcatel-Lucent support representative, as described in Procedure 10-1.

9 — Troubleshooting using the 5620 SAM user activity log

9.1 Troubleshooting using the 5620 SAM user activity log overview

The 5620 SAM user activity log allows an operator to view information about the actions performed by each 5620 SAM GUI and OSS user.

Note — A 5620 SAM operator with an Administrator scope of command role can view all user activity log records except records associated with LI management. Viewing LI management records requires the Lawful Intercept Management role.

You can use the User Activity form to do the following:

- List and view information about recent user activities.
- List and view information about recent user sessions and the actions performed during each session.
- Navigate directly to the object of a user action.
- View 5620 SAM client session information that includes connection, disconnection, and authentication failure events.
- View 5620 SAM server session information, that includes startup, shutdown, and access violation events.

Note — The 5620 SAM also raises an alarm for a security-related event such as an authentication failure or access violation.

You can navigate directly from an object properties form to a filtered list of the activities associated with the object. See the *5620 SAM User Guide* for more information about the user activity log and using the User Activity form.

Table 9-1 lists the troubleshooting procedures associated with the user activity log.

Table 9-1 Troubleshooting with the client activity log

Problem	Solution
To identify the user activity for a network object	Procedure 9-1
To identify the user activity for a 5620 SAM object	Procedure 9-2
To navigate to the object of a user action	Procedure 9-3
To view the user activity records of an object	Procedure 9-4
To view the user activity performed during a user session	Procedure 9-5

Note — Ther User Activity form and related list forms do not refresh dynamically. To view the latest log entries in a list form, you must click on the Search button.

Each log entry has a request ID. There can be multiple log entries associated with a single request ID. For example, the creation of a discovery rule that has multiple rule elements creates one log entry for each rule element. You can use the request ID to sort and correlate the multiple log entries associated with a single client operation.

9.2 Troubleshooting using the 5620 SAM User Activity procedures

The following procedures describe how to use the 5620 SAM user activity log functions to determine whether a user action is the cause of a problem.

Procedure 9-1 To identify the user activity for a network object

1. Open the User Activity form.
2. Click on the Activity tab.
3. Specify the filter criteria for the object.
4. Click on the Search button. A list of user activity entries is displayed.
5. View the State column values for the activities associated with the object. A value of Failure or Timeout means that the action did not modify the object. A value of Success represents the successful deployment of the configuration action.
6. To view a suspect entry, such as a failed or incorrect configuration attempt, select the required entry and click on the Properties button. The Activity form opens.
7. Use the activity information from one or more entries to determine whether a sequence of user actions is the source of the problem.
8. Close the open forms, as required.

Procedure 9-2 To identify the user activity for a 5620 SAM object

1. Open the User Activity form.
2. Click on the Activity tab.
3. Specify a Site Name of NONE as the filter criterion.
4. Click on the Search button. A list of user activity entries is displayed.
5. Sort the entries to locate the affected 5620 SAM object.
6. View the State column values for the activities associated with the object. A value of Failure or Timeout means that the action did not modify the object. A value of Success means that the object modification succeeded.
7. To view an entry, select the required entry and click on the Properties button. The Activity form opens.

8 Use the activity information from one or more entries to determine whether a sequence of user actions is the source of the problem.

9 Close the open forms, as required.

Procedure 9-3 To navigate to the object of a user action

1 Open the User Activity form.

2 Click on the Activity tab.

3 Specify the filter criteria, if required.

4 Click on the Search button. A list of user activity entries is displayed.

5 Select an entry and click on the Properties button. The Activity form opens.

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

7 Close the open forms, as required.

Procedure 9-4 To view the user activity records of an object

1 Open the required object properties form.

2 Click on the User Activity button, or, if the button is not displayed, click on the More Actions button and choose User Activity. The User Activity form opens and displays a filtered list of user activity records associated with the object.

3 To view an entry, select the entry and click on the Properties button. The Activity form opens.

4 Close the open forms, as required.

Procedure 9-5 To view the user activity performed during a user session

1 Open the User Activity form.

2 Specify the filter criteria, if required.

3 Click on the Search button. A list of user session entries is displayed.

4 Select an entry and click on the Properties button. The Session form opens with the General tab displayed.

5 Click on the Activity tab.

6 Specify the filter criteria, if required.

7 Click on the Search button. A list of the actions performed by the user during the session is displayed.

8 To view an entry, select the entry and click on the Properties button. The Activity form opens.

9 Close the open forms, as required.

Troubleshooting the 5620 SAM platform, database, server, or clients

10 — Troubleshooting the 5620 SAM platform

10.1 Troubleshooting the 5620 SAM platform

Table 10-1 describes the problems or tasks associated with troubleshooting 5620 SAM platform issues.

Table 10-1 5620 SAM platform problems or tasks

Problem	Solution
To collect the 5620 SAM log files	Procedure 10-1
Problem: Poor performance on a RHEL or Solaris station	Procedure 10-2
Problem: Device discovery fails because of exceeded RHEL ARP cache	Procedure 10-3

10.2 Troubleshooting the 5620 SAM platform procedures

The following procedures describe how to troubleshoot the 5620 SAM platform.

Procedure 10-1 To collect the 5620 SAM log files

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

When a 5620 SAM log file reaches a predetermined size, the 5620 SAM closes, compresses, and renames the file by including a sequence number and a timestamp. The following is an example of the filename format:

EmsServer.#.*timestamp*.log

where

is a sequence number; the sequence begins at 0

timestamp is the time of closure, in the following format: YYYY-MM-DD_hh-mm-ss

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

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

i Log on to the station as the root user.

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

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

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

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

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

2 For a database problem that is not related to installation, perform the following steps:

   i Log on to the station as the Oracle management user.

   ii Collect the following files:

   - *install_dir*/config/dbconfig.properties
   - all files in *install_dir*/admin/diag/rdbms/*instance_name*/*instance_name*/alert
   - all files in *install_dir*/admin/diag/rdbms/*instance_name*/*instance_name*/trace
   - all files in *install_dir*/admin/diag/proxy
   - all files with a .log extension in the following directories:
     - *install_dir*
     - *install_dir*/config

   where
   install_dir is the database installation location, typically /opt/5620sam/samdb/install
   instance_name is the database instance name, typically samdb in a standalone deployment, or samdb1 or samdb2 in a redundant deployment

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

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

   where *install_dir* is the main server installation location, typically /opt/5620sam/server

   On an auxiliary server, log files are found in the following directories:

   - *install_dir*/nms/log
   - *install_dir*/nms/jboss/server/auxiliary/log

   where *install_dir* is the auxiliary server installation location, typically /opt/5620sam/auxserver

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

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

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

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

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

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

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

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

ii Open a console window.

iii Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin on a main server, or /opt/5620sam/auxserver/nms/bin on an auxiliary server.

iv Enter the following at the prompt:

getDebugFiles.bash *output_dir days* ↵

where
output_dir is a local directory that is to contain the output files
days is the number of days for which to collect log files, beginning with the most recent

Note 1 — You cannot specify /tmp, or any directory below /tmp, as the output directory.

Note 2 — The *days* parameter is optional.

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

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

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

viii Enter the following at the prompt:

getSAMDebugFiles.bash *output_dir days* ↵

where
output_dir is a local directory that is to contain the output files
days is the number of days for which to collect log files, beginning with the most recent

Note 1 — You cannot specify /tmp, or any directory below /tmp, as the output directory.

Note 2 — The *days* parameter is optional.

ix Collect the following output files:

- the *hostname*.WsInfoFiles.tar.gz file, which contains basic server or database station information, such as the networking configuration
- on a server station, the *hostname*.ServerLogFiles.tar.gz file, which contains server and JBoss logs and configuration information
- on the database station, the *hostname*.DBLogFiles.tar.gz file, which contains database logs and configuration information

where *hostname* is the station hostname

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

8 Send the files to Alcatel-Lucent technical support, as required.

Procedure 10-2 Problem: Poor performance on a RHEL or Solaris station

When a station is taking too long to perform a task, you can check the CPU status to ensure that one process is not using most of the CPU resources, and then use commands to review the CPU usage.

When CPU usage remains high and performance degrades, contact Alcatel-Lucent technical support. Provide the data that you collect when you perform this procedure.

You can also perform other procedures to monitor performance: 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 14-3.

1 Log on to the station as the root user.

2 Open a console window.

3 If the station OS is Solaris, go to step 7.

4 Perform the following steps to check for processes that are consuming excessive CPU cycles:

i To list the top CPU processes using the UNIX utility prstat, type:

```
# top ↵
```

Depending on your system configuration, approximately the top 20 processes are displayed.

ii Review the output.

The top 5620 SAM process in the CPU column should be the Java process. However, the Java process should not be consuming too much CPU. Some Oracle processes may also consume CPU, depending on the database load.

iii Press CTRL-C to stop the command.

5 Perform the following steps to view a CPU activity summary.

i Enter the following command:

```
# mpstat time ↵
```

where *time* is the interval, in seconds, between CPU polls; a value between 10 and 60 is recommended

ii Review the command output. Code 10-1 is an example of RHEL mpstat output; Table 10-2 describes each output field.

Code 10-1: RHEL mpstat output example

```
CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest   %idle
all    0.25    0.00    0.17    0.00    0.00    0.00    0.00    0.00   99.58
all    0.50    0.00    0.08    0.08    0.00    0.00    0.00    0.00   99.33
all    0.17    0.00    0.08    0.00    0.00    0.00    0.00    0.00   99.75
all    0.25    0.00    0.17    0.08    0.00    0.00    0.00    0.00   99.50
```

Table 10-2 RHEL mpstat field descriptions

Heading	Description (events per second unless noted)
CPU	Processor number; the keyword all indicates that statistics are calculated as averages among all processors
%usr	Percentage of CPU utilization at the user application level
%nice	Percentage of CPU utilization at the user level with nice priority
%sys	Percentage of CPU utilization at the system level; does not include time spent servicing hardware and software interrupts
%iowait	Percentage of CPU idle time during which the system had an outstanding disk I/O request
%irq	Percentage of CPU time spent servicing hardware interrupts
%soft	Percentage of CPU time spent servicing software interrupts
%steal	Percentage of time spent in involuntary wait by the virtual CPU or CPUs during hypervisor servicing of another virtual processor
%guest	Percentage of CPU time spent running a virtual processor
%idle	Percentage of CPU idle time without an outstanding disk I/O request

Review the %usr, %sys and %idle statistics, which together indicate the level of 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.

iii Press CTRL-C to stop the command.

6 Go to step 9.

7 Perform the following steps to check for processes that are consuming excessive CPU cycles:

i To list the top CPU processes using the UNIX utility prstat, type:

```
# prstat ↵
```

Depending on your system configuration, approximately the top 20 processes are displayed.

ii Review the output.

The top 5620 SAM process in the CPU column should be the Java process. However, the Java process should not be consuming too much CPU. Some Oracle processes may also consume CPU, depending on the database load.

iii Press CTRL-C to stop the command.

8 Perform the following steps to view a CPU activity summary.

i Enter the following command:

```
# mpstat time ↵
```

where *time* is the interval, in seconds, between CPU polls; a value between 10 and 60 is recommended

ii Review the command output. Code 10-2 is an example of Solaris mpstat output; Table 10-3 describes each output field.

Code 10-2: Solaris mpstat output example

```
CPU minf mjf xcal  intr ithr  csw icsw migr smtx  srw syscl  usr sys  wt idl
  0   10   0  442  302  419   166   12  196    0  775    95    5   0   0  95
  1    1   0  220  237  100   383  161   41   95    0   450   96   4   0   0
  2    0   0   27  192  100   178   94   38   44    0   100   99   1   0   0
  3    1   0  160  255  100   566  202   28  162    0  1286   87   8   0   5
```

Table 10-3 Solaris mpstat field descriptions

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

(1 of 2)

Heading	Description (events per second unless noted)
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 CTRL-C to stop the command.

9 If processes are competing for CPU resources, perform the following steps to isolate the information about a single process.

i Check the state of CPUs by typing:

ps -aux ↵

A list of processes is displayed.

ii Review the command 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 CTRL-C to stop the command.

Procedure 10-3 Problem: Device discovery fails because of exceeded RHEL ARP cache

When a 5620 SAM system on RHEL manages a large number of NEs in a broadcast domain the ARP cache may fill and prevent the discovery of additional devices. When this happens, the /var/log/messages file contains entries like the following:

```
Jan 21 09:37:40 hostname kernel: Neighbour table overflow

Jan 21 09:37:40 hostname kernel: Neighbour table overflow

Jan 21 09:37:40 hostname kernel: Neighbour table overflow

Jan 21 09:38:00 hostname kernel: __ratelimit:190 callbacks suppressed
```

Perform this procedure when one of the following occurs:

- The /var/log/messages file contains more than 1024 entries.
- You need to increase the ARP cache size to accommodate the network.

The default ARP cache threshold values are the following:

- Threshold 1—128
- Threshold 2—512
- Threshold 3—1024

1 Log in to the main server station as the root user.

2 Open a console window.

3 Perform one of the following to increase the ARP cache thresholds.

a To temporarily increase the thresholds, type the following:

```
# echo 8096 > /proc/sys/net/ipv4/neigh/default/gc_thresh1 ↵
# echo 25600 > /proc/sys/net/ipv4/neigh/default/gc_thresh2 ↵
# echo 32384 > /proc/sys/net/ipv4/neigh/default/gc_thresh3 ↵
```

b To permanently override the default thresholds, perform the following steps.

i Open the /etc/sysctl.conf file using a plain-text editor such as vi.

ii Locate the following comment line:

```
#========= 5620 SAM: Info begins =========
```

iii Add the following after the comment line:

```
net.ipv4.neigh.default.gc_thresh1 = 8096
net.ipv4.neigh.default.gc_thresh2 = 25600
net.ipv4.neigh.default.gc_thresh3 = 32384
```

iv Save and close the file.

v Enter the following:

```
# sysctrl -p ↵
```

4 Close the console window.

11 — Troubleshooting with the 5620 SAM LogViewer

11.1 5620 SAM LogViewer overview

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

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

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

LogViewer can interpret the various 5620 SAM log-file formats. The log files must be local server or database logs.

Table 11-1 describes the tasks associated with troubleshooting the 5620 SAM using the LogViewer.

Table 11-1 5620 SAM LogViewer

Problem or task	Solution
To display logs using the LogViewer GUI	Procedure 11-1
To configure the LogViewer application using the GUI	Procedure 11-2
To search log files in a path	Procedure 11-3
To show or hide buttons from the LogViewer main tool bar	Procedure 11-4
To set highlight colors and fonts for LogViewer components and levels	Procedure 11-5
To automatically show or hide log messages	Procedure 11-6
To manage filters using the GUI Filter Manager	Procedure 11-7
To specify a plug-in using the LogViewer GUI	Procedure 11-8
To display logs using the LogViewer CLI	Procedure 11-9
To configure the LogViewer CLI	Procedure 11-10
To specify plug-ins using the CLI	Procedure 11-11

Configuration

The LogViewer GUI and CLI applications share a set of configuration options; changes made to these options by one application affect the other. Other options apply to the GUI only.

You can customize LogViewer by creating and saving log filters and log profiles that are available to all GUI and CLI users, and can save the GUI application configuration, or workspace, to have LogViewer display the currently open logs the next time it starts. LogViewer does not save the current filter and display configuration for a log when you close the log unless you export the configuration to a log profile.

Your operating configuration of LogViewer is stored in the user directory. Any filters, fonts, colors, or other preferences you have set such as location, size and splitter location, are used the next time you start the application.

For multiple instances of LogViewer running on the same server, you can set the system environment variable LOGV_HOME to make all instances use the same properties file. In this way, properties such as filters, window location, and window size are common to all instances.

Filters

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

Plug-ins

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

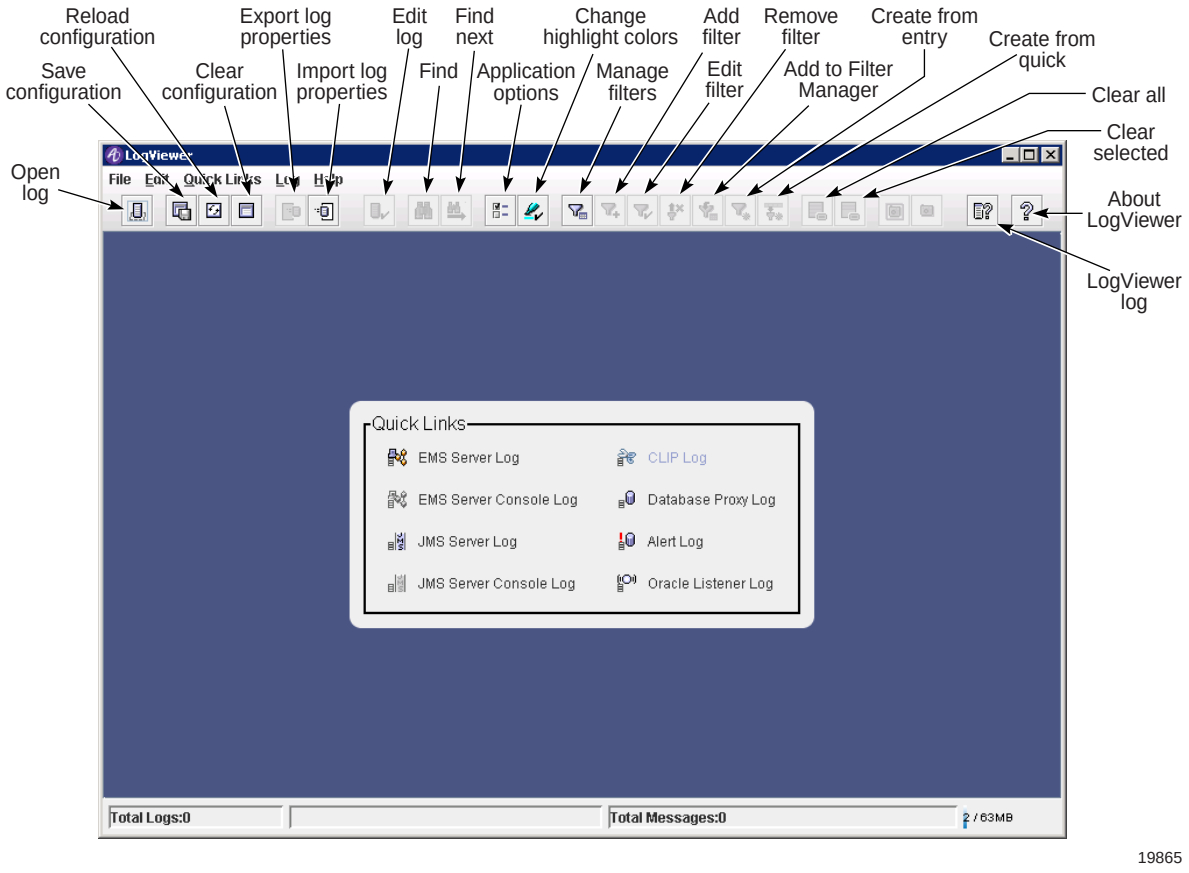
LogViewer has default plug-ins that can send notifications, such as e-mail messages and GUI pop-ups, when a new log entry matches a set of filter criteria. The LogViewer e-mail plug-in uses SMTP as the transport.

11.2 LogViewer GUI

The LogViewer GUI opens to display a Quick Links panel that has shortcuts to the logs that are present on the local file system. When you click on a log shortcut, LogViewer opens a tab that displays the most recent log entries. Figure 11-1 shows the LogViewer GUI with the Quick Links panel displayed and describes the main tool bar buttons.

Note — If you hover your cursor over a GUI tab or field, a description or configuration instruction specific to that tab or field will appear.

Figure 11-1 LogViewer GUI showing Quick Links panel

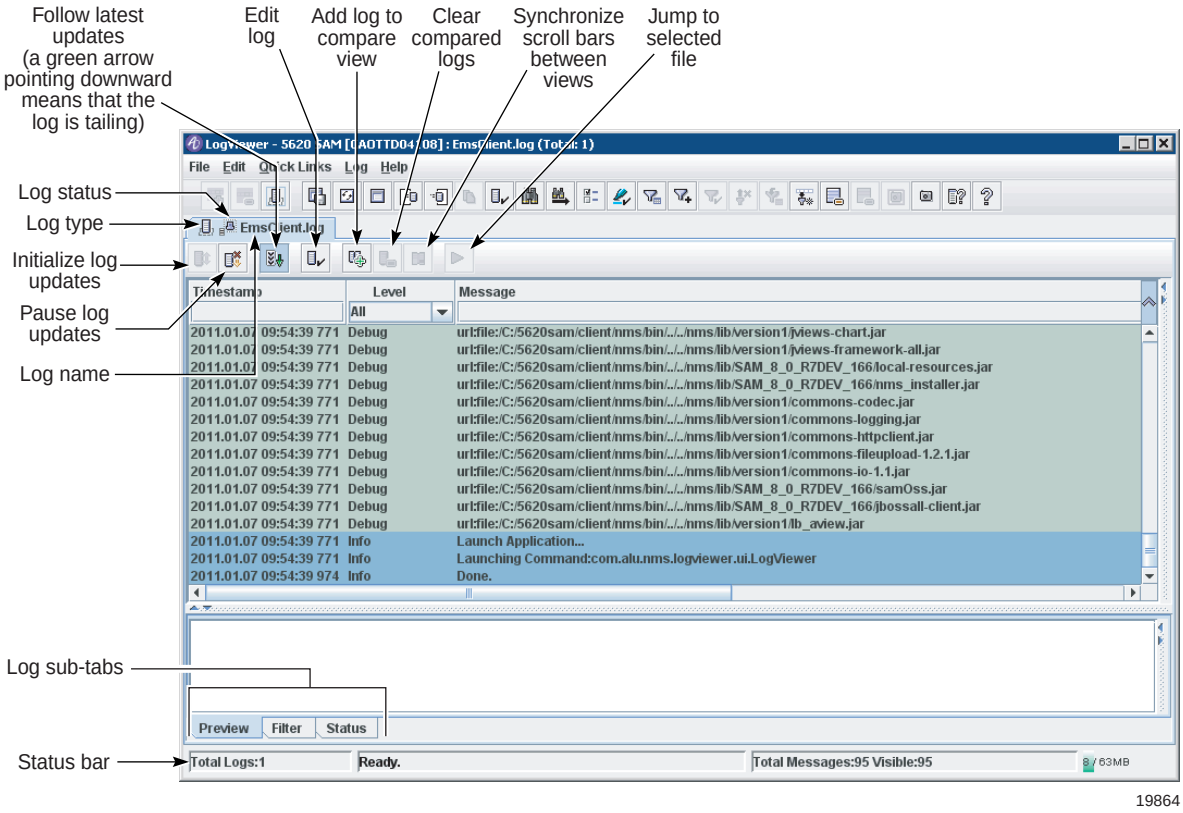


Overview

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

Figure 11-2 shows the LogViewer GUI with multiple open logs and describes the tool bar buttons on a tab that displays a currently active log.

Figure 11-2 LogViewer GUI showing log tabs



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

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

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

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

GUI-based log filtering

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

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

You can also create and use simple filters. These filters do not require the use of regular expressions, but instead, perform a case insensitive "contains" filtration of a string you specify. The use of simple filters must be enabled using the Preferences→Options menu option.

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

11.3 LogViewer CLI

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

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

11.4 LogViewer GUI procedures

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

Procedure 11-1 To display logs using the LogViewer GUI

Perform this procedure to start the LogViewer GUI application and view one or more logs. See Figures 11-1 and 11-2, or move the mouse cursor over a GUI object, to view a description of the object, for example, a tool bar button.

1. Log in to the 5620 SAM server as the samadmin user.
2. Open a console window.
3. Enter the following at the prompt:

   bash$ ***path*/nms/bin/logviewerui.bash** ↵

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

i Choose one of the following options:

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

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

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

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

Common display operations

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

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

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

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

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

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

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

Note — The LogViewer Find function does not support the use of regular expressions. To perform a search using a regular expression, use the Find In Path function, as described in Procedure 11-3.

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

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

v Close the Find form if it is open.

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

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

- **a** To clear all listed log entries, choose Log→Clear All Events from the LogViewer main menu, or click on the Clear all button in the main tool bar.
- **b** To clear the currently selected log entries, choose Log→Clear Selected Events from the LogViewer main menu, or click on the Clear selected button in the main tool bar.
- **c** To clear all log entries that match the currenly selected cell, select a cell and choose Log→Hide All Like Selected from the LogViewer main menu, or click on the Hide All Like Selected button in the main tool bar.
- **d** To show only log entries that match the currently selected cell, select a cell and choose Log→Show All Like Selected from the LogViewer main menu, or click on the Show All Like Selected button in the main tool bar.

11 To apply a quick filter, enter a regular expression as a match criterion in the field below a column header and press ↵. The list is cleared, and only subsequent log entries that match the criterion are displayed. See Procedure 11-7 for more information about using filters.

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

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

- **i** Choose Log→Add Filter from the LogViewer main menu, or click on the Add filter button in the main tool bar. The Select Filters form opens.
- **ii** Select one or more filters in the list and click on the OK button. The filters are applied to the log view and are listed on the Filters sub-tab of the log tab.

  See Procedure 11-7 for information about creating saved filters.

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

15 If the log display is static, such as for an archived log or the result of a Find All operation, go to step 22.

Dynamic view operations

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

- **i** Configure the Max. Messages parameter to specify the maximum number of entries that are listed on the log tab. LogViewer removes the oldest entries as required to keep the number of entries at or below this value.
- **ii** Configure the Auto-Tail parameter to specify whether the log tab dynamically displays the log updates.
- **iii** Click on the OK button to close the Local Log File form.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Static view operations

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

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

23 To copy the text of selected log entries to the clipboard, select one or more log entries in a log tab and choose Edit→Copy from the LogViewer main menu, or click on the Copy button in the main tool bar.

24 To save selected log entries to a file, select one or more log entries in a log tab and click on the Save Selected button in the main tool bar.

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

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

Procedure 11-2 To configure the LogViewer application using the GUI

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

1 Open the LogViewer GUI.

2 Choose Edit→Options→General from the LogViewer main menu, or click on the Application options button in the main tool bar. The Options form opens with the General tab displayed.

3 Configure the parameters:

- Last Directory—Click in the parameter field and use the browser form that opens to specify where to save exported log profiles.
- Base File Messages Directory—Click in the parameter field and use the browser form that opens to specify the base 5620 SAM log directory.
- Default Character Set—Edit this parameter to specify the character set that LogViewer uses to display the log-file contents.
- Default Log Pattern—Edit this parameter to specify a regular expression that LogViewer uses to interpret log-file contents.
- Default Date Format—Enter a colon-separated string to specify the LogViewer date format using y for year digits, M for month digits, d for date digits, H for hour digits, m for minute digits, s for second digits, and S for millisecond digits, for example, yyyy:MM:dd HH:mm:ss:SSS.
- Regular Expression Help URL—Enter a value to specify the location of the Java regular-expression help web page that opens when you click on the Help button while testing a regular expression for a filter.
- Web Browser Location—Enter a value to specify the location of the local file browser used to open the Java regular-expression help web page.
- Quick Links Refresh Time (ms)—Enter a value to specify how often LogViewer refreshes the Quick Links list.
- Rollover Remove Size—Enter a value to specify the number of log entries to remove from the LogViewer display when the maximum number of displayed log entries is reached.
- Delay for local file polling (ms)—Enter a value to specify, in ms, how long LogViewer waits before it checks local log files for updates.
- Hide Table Tooltips—Select this parameter to suppress the display of tool tips when the mouse pointer moves over log entries in a log tab.
- Use Simple Filters—Select this parameter to allow the use of simple filters.
- Advanced Quick Filter—Select this parameter to display the advanced Quick Filter table header on log tabs.
- Display Advanced Quick Filter—Select this parameter to display the advanced Quick Filter table header on the log tab when a log file is opened.
- Include Host in Title—Select this parameter to display the hostname in the log title.
- Show Memory Monitor—Select this parameter to display the memory monitor at the bottom right corner of the LogViewer window.
- Memory Monitor Clear Messages—Select this parameter to allow the memory monitor to attempt recovery by clearing some messages from live event logs when the memory threshold is exceeded.
- Clear Log on Rollover—Select this parameter to clear the events from the logs when a Style View file rolls over or is moved.
- Style View—Select this parameter to display the styled preview pane.
- Memory Monitor Threshold (%)—Enter a value to specify the percentage of available memory that LogViewer uses before it stops displaying log updates.
- Max. Recent Files—Enter a value to specify the number of files that LogViewer keeps in the list of recently opened files.
- Max. Profile Files—Enter a value to specify the number of profile files that LogViewer keeps in the list of recently opened files.
- LogViewer Log Level—Choose a logging level from the drop-down menu to specify the minimum log level of the LogViewer application messages.

- Enable Viewer Performance Stats—Select this parameter to enable the display of LogViewer performance statistics.
- Stats Timer (seconds)—Enter a value to specify the number of seconds that LogViewer waits between log statistics updates.

4 Click on the Command Line tab to configure the LogViewer CLI application.

5 Configure the following parameter:

- Command line buffer size—Enter a value to specify the number of log messages that LogViewer buffers when the CLI application is in command mode.

6 Choose an ANSI display attribute from the drop-down menu beside each of the following parameters to specify how the CLI application displays the corresponding text.

- Normal Display—for normal application text
- Trace Level Display—for trace-level log entries
- Debug Level Display—for debug-level log entries
- Info Level Display—for info-level log entries
- Warning Level Display—for warning-level log entries
- Error Level Display—for error-level log entries
- Fatal Level Display—for fatal-level log entries
- Filter Display—for filtered log entries

7 Configure the Always Use ANSI Display parameter, as required.

8 Click on the 5620 SAM tab to configure the parameters that are specific to the 5620 SAM.

9 Configure the following parameters by clicking in the parameter field and using the browser form that opens to specify a directory:

- Database Location—specifies the base 5620 SAM database installation directory
- Oracle Location—specifies the base 5620 SAM Oracle installation directory
- NMS Root—specifies the nms directory under the base 5620 SAM server installation directory

Note — Your configuration of LogViewer is stored in the user directory. Any filters, fonts, colors, or other preferences you have set are preserved when you install a newer version of the application. However, if you install the server in a different location, LogViewer cannot display the quick links properly. To correct this, configure the NMS Root parameter to specify the new server location.

10 Click on the Advanced tab to configure the parameters related to LogViewer performance.

Caution — The parameters on the Advanced tab typically require configuration only when LogViewer has performance problems. Consult Alcatel-Lucent technical support before you attempt to modify a parameter on the Advanced tab, as it may affect server performance.

Procedure 11-3 To search log files in a path

Use this procedure to perform a search on all log files in a specified path using a plain text search or a regular expression.

Note — You can test regular expressions in the Find In Path window by clicking on the Test button beside the expression. Enter sample text in the Example box, and an expression in the Expression box, then click on the green Execute button to test the results of the expression.

1 Open the LogViewer GUI.

2 Choose Edit→Find In Path from the LogViewer main menu, or click on the Search all files button. The Find In Path window opens.

3 Perform one of the following:

a To perform a text search, specify the text string to search for in the Text to find parameter and deselect the Regular expression option.

b To perform a search using a regular expression, enter a regular expression in the Text to find parameter and select the Regular expression option.

4 In the Directory parameter, enter the directory path you need to search, or click on the Browse button and select a directory. To search subdirectories, select the Recursive option.

5 To restrict the search to logs with certain filenames, enter a regular expression in the File Mask parameter. To search all logs in the specified path, leave this parameter blank.

6 Click on the Find button. The log entries matching the search parameters are displayed in a new tab.

Note — A new search using the Find In Path function cannot be performed until the search tab is closed.

Procedure 11-4 To show or hide buttons from the LogViewer main tool bar

Perform this procedure to show or hide specific buttons from the LogViewer main tool bar.

1 Open the LogViewer GUI.

2 Choose Edit→Preferences→Manage Toolbar from the LogViewer main menu. The Manage Toolbar page opens divided into a Palette and Toolbar section.

3 Use the directional arrows to manage which buttons appear in the main tool bar, and the order in which the buttons appear.

4 Click on the OK button to save your settings.

Procedure 11-5 To set highlight colors and fonts for LogViewer components and levels

Perform this procedure to set highlight colors and fonts for the various LogViewer components and levels.

1 Open the LogViewer GUI.

2 Choose Edit→Preferences→Highlight Colors from the LogViewer main menu. The Highlight Color Selection form opens.

3 Set the item for which you want to specify colors and/or fonts by choosing it from the Component/Level drop-down menu.

4 For the item that you want to change, choose the foreground or background plane as required, by clicking on the appropriate tab. The foreground is the text contained in a field. The background is the fill color of the field behind the text.

5 For foreground text items, set the font type, style, and size, as required.

6 For either foreground or background items, set the color as required. You can choose a color from the samples shown on the Swatch tab, or you can specify a color by entering its red, green, and blue values in the RGB tab.

Previews of your choices appear in the sample fields at the bottom of the form.

7 Click on the OK button to save your settings.

Procedure 11-6 To automatically show or hide log messages

Perform this procedure to automatically filter (show or hide) log messages based on the current selected cell in the message table.

1 Open the LogViewer GUI.

2 To automatically show or hide log messages, perform the following steps.

i Select a log entry.

ii To hide log messages based on a selected cell in the message table, perform one of the following:

- Right-click on the cell and choose Hide All Like Selected.
- Choose Log→Hide All Like Selected from the LogViewer main menu.
- Click the Hide All Like Selected button in the main tool bar.

LogViewer hides all messages that contain the selected cell. For example, if you have selected the cell in the “Logger” column that contains the word “samConsole”, all messages that have the logger set to “samConsole” are hidden.

iii Perform one of the following to show log messages based on a selected cell in the message table.

- Right-click on the cell and choose Show All Like Selected.
- Choose Log→Show All Like Selected from the LogViewer main menu.
- Click the Show All Like Selected button in the main tool bar.

This shows all messages that contain the selected cell. For example, if you have selected the cell in the “Logger” column containing the word “samConsole”, all messages that have the logger set to “samConsole” are displayed.

Procedure 11-7 To manage filters using the GUI Filter Manager

Perform this procedure to create, modify, assign or delete a LogViewer filter.

Note — The Filter Manager is opened from within LogViewer, but runs as a separate applet. This enables the dragging and dropping of filters between Filter Manager and the Filters sub-tab of a lob tab.

1 Choose Log→Filter Manager from the LogViewer main menu. The Filter Manager applet opens.

2 To add a regular filter or a simple filter, perform the following steps:

i Click on the Add or Add Simple button, as required. The Add Filter form opens.

ii Configure the Name parameter by specifying a unique name for the filter.

iii Configure the following parameters that correspond to the fields in a log entry by entering regular expressions for regular filters, or just strings for simple filters as a filter criterion for each:

- Level
- Message
- Thread
- Logger
- Timestamp
- Platform

iv If you are configuring a simple filter, go to step 2 xi.

v Test a regular expression that you enter by clicking on the Test button beside the regular expression. The Regular Expression form opens.

vi Paste an example log entry that you want to match using the regular expression into the Example field.

vii Click on the green right-pointing arrow to test the expression. If the expression is invalid, a message is displayed to indicate the error in the expression.

viii Correct the errors in the expression.

ix Repeat steps 2 vii and 2 viii until no error message is displayed.

x Repeat steps 2 v to 2 ix to test additional regular expressions, if required.

xi Enable the Color parameter and click in the field beside the parameter to specify a highlight color for the matching log entries. A standard color chooser form opens.

xii Use the form to specify a color and click on the OK button. The color chooser form closes and the Add Filter form reappears.

xiii Click on the OK button. The Add Filter form closes and the Filter Manager form lists the new filter.

3 To create a saved filter based on the current quick filter, perform the following steps.

- **i** Choose Log→Create from Quick Filter from the LogViewer main menu, or click on the Create from quick button in the main tool bar. The Add Filter form opens and is populated with the quick filter match criteria.
- **ii** Modify the match criteria as required.
- **iii** Click on the OK button to save the filter.

4 To create a saved filter using a log entry as a template, perform the following steps.

- **i** Select a log entry.
- **ii** Choose Log→Create from Selected from the LogViewer main menu, or click on the Create from entry button in the main tool bar. The Add Filter form opens and is populated with the current log-entry field values as match criteria.
- **iii** Modify the match criteria as required.
- **iv** Click on the OK button to save the filter.

5 To move a filter to other instances of the LogViewer, perform the following steps.

- **i** To export a filter, click the Export button in the main tool bar, or choose Log→Filter Manager from the LogViewer main menu. The Export form opens, and allows you to export a filter to a specified file.
- **ii** To import a filter, click the Import button in the main tool bar, or choose Log→Filter Manager from the LogViewer main menu. The Import form opens, and allows you to import a filter from a specified file.
- **iii** Click on the OK button to save the filter.

6 To make a copy of a filter, select the filter and click on the Copy button. A copy of the filter is listed on the Filter Manager form.

7 To edit a filter, select the filter and click on the Edit button. Configure the parameters described in step 2.

8 To delete a filter, select the filter and click on the Delete button

Procedure 11-8 To specify a plug-in using the LogViewer GUI

Perform this procedure to configure and enable plug-ins for a log file.

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

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

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

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

4 Click on the Plugins tab.

5 Choose a plug-in from the Plugin drop-down menu.

6 If you choose the Bring to Front plug-in, perform the following steps.

i Specify a regular expression as a match criterion in the Message Filter field.

ii Go to step 8.

7 If you choose the E-Mail plug-in, perform the following steps.

i Specify a regular expression as a match criterion in the Message Filter field.

ii Configure the parameters:

- Message Filter—specifies a regular expression that is used as a filter to identify the log entries that invoke the plug-in
- Subject—specifies the e-mail message subject line
- Body Prefix—specifies the text that precedes the log-entry text in an e-mail message
- Authenticate? —specifies whether or not authentication is enabled
- User—specifies a user name associated with the plug-in
- Password—specifies an SMTP password
- Host—specifies the name of an SMTP e-mail server
- Use TLS? —specifies whether the mailbox server needs to use Transport Layer Security (TLS) encryption
- Use SSL? —specifies whether the mailbox server needs to use Secure Sockets Layer (SSL) encryption
- To—specifies the e-mail address of the recipient
- From—specifies the sender e-mail address used by the plug-in
- Minimum E-mail Time (minutes)—specifies the minimum time between messages that the plug-in sends, to prevent e-mail flooding

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

11.5 LogViewer CLI procedures

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

Procedure 11-9 To display logs using the LogViewer CLI

Perform this procedure to start the LogViewer CLI application and view one or more logs.

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

2 Open a console window.

3 Enter the following at the prompt:

bash$ ***path*/nms/bin/logviewer.bash *argument options parameter*** ↵

where
path is the 5620 SAM server installation location, typically /opt/5620sam/server
argument is an argument listed in Table 11-2
options is one or more of the options listed in Table 11-3
parameter is a parameter listed in Table 11-4

Table 11-2 LogViewer CLI startup arguments

Argument	Meaning
--version	Display LogViewer version information.
--help	Display LogViewer CLI help text.

Table 11-3 LogViewer CLI startup options

Option	Meaning
-counter	Prepend a counter number to each displayed log entry.
-parseAll	Parses and display the entire contents of a file before displaying the real-time updates.
-ansi *level attribute*	Display events and filters using ANSI-specified colors where *level* is a logging level, such as debug *attribute* is an ANSI color attribute, such as 42m to specify the color green
-quit	Quit LogViewer after parsing the log files.

Table 11-4 LogViewer CLI startup parameters

Parameter	Meaning
-xml *file_name*	Read information such as log file, plug-in and filter specifications from the XML file specified by *file_name*. The LogViewer GUI can export this information to an XML file.
file name	Display the specified file when LogViewer starts.

The LogViewer CLI opens in display mode. If a log file is specified as a startup parameter, the most recent entries in the log file are displayed as they are written to the log file. Otherwise, a cursor is displayed.

4 Enter command mode by pressing ↵. The following prompt is displayed:

```
log>
```

This prompt is called the root prompt. Table 11-5 describes the options that are available at the root prompt.

Table 11-5 LogViewer CLI root menu options

Option	Function
open	opens a submenu for choosing the logs to view
include	opens a submenu for specifying which log files to list in the *open* submenu
filter	opens a submenu for adding, listing or deleting filters
plugin	opens a submenu for adding, listing or delete plugins
options	opens a submenu for configuring LogViewer CLI and GUI application options
list	lists the files in the *open* submenu file list
reset	resets the log message counts
stats	displays LogViewer statistics for the current log
The following options are also available in submenus:	
back	goes to the previous menu
root	goes to the root menu
quit	quits the application
return	returns to display mode

5 Enter the following at the prompt:

open ↵

The following prompt is displayed:

```
log-open>
```

6 Press ↵ to display the list of available logs.

7 Perform one of the following.

a To view a log in the list, enter the name of a log at the prompt and press ↵.

b To view a log that is not listed, perform the following steps.

i Enter the following at the prompt:

other ↵

The following prompt is displayed:

```
File Name (full path)?
```

ii Enter the absolute or relative path of the log file that you want to open and press ↵. LogViewer opens the file.

8 Enter the following at the prompt to enter display mode and view the real-time log updates:

`return` ↵

LogViewer enters display mode. Log updates are displayed as they occur.

9 To add a filter that restricts the types of log entries that are displayed during the current LogViewer session, perform the following steps.

i Press ↵ to enter command mode.

ii Enter the following at the prompt to return to the root menu:

`root` ↵

The following prompt is displayed:

```
log>
```

iii Enter the following at the prompt:

`filter` ↵

The following prompt is displayed:

```
log-filter>
```

Note — You can also use commands at this menu level to list and delete filters.

iv Enter the following at the prompt:

`add` ↵

The following prompt is displayed:

```
Filter name:
```

v Enter a name for the filter and press ↵.

vi The following prompts are displayed in sequence:

```
Level:

Logger:

Thread:

Timestamp:

Message:
```

At each prompt, enter a regular expression to use as a match criterion, if required, and press ↵.

vii The following prompt is displayed:

```
Display Filter? (Y/N):
```

Enter y ↵ to apply the filter to the current log display. LogViewer applies the filter.

viii Enter the following to return to display mode:

`return` ↵

LogViewer enters display mode. The log updates are filtered before they are displayed.

10 To list the available log files, perform the following steps.

i Press ↵ to enter command mode.

ii Enter the following at the prompt:

`list` ↵

LogViewer lists the available log files.

iii Enter the following at the prompt to return to display mode:

`return` ↵

11 To display statistics about the current LogViewer session, perform the following steps.

i Press ↵ to enter command mode.

ii Enter the following at the prompt:

`stats` ↵

LogViewer displays statistics about the current session.

iii Enter the following at the prompt to return to display mode:

`return` ↵

12 To reset the statistics counters for the current LogViewer session, perform the following steps.

i Press ↵ to enter command mode.

ii Enter the following at the prompt:

`reset` ↵

LogViewer resets the counters.

iii Enter the following at the prompt to return to display mode:

`return` ↵

13 Enter the following at the prompt to close LogViewer:

`quit` ↵

Procedure 11-10 To configure the LogViewer CLI

Perform this procedure to use the LogViewer CLI to configure general CLI application options.

Note — The options configured in this procedure apply only to the current LogViewer CLI session.

1 Open the LogViewer CLI.

2 To add a file to the list of files in the *open* menu, perform the following steps.

i Press ↵ to enter command mode.

ii Enter the following at the root prompt:

`include` ↵

The following prompt is displayed:

```
log-include>
```

iii Enter the following at the prompt:

`add` ↵

The following prompt is displayed:

```
File Name (full path)?
```

iv Enter the absolute or relative path of the log file that you want to add and press ↵. LogViewer adds the file to the list in the *open* menu.

Note — The LogViewer CLI supports file drag-and-drop functionality.

v Enter the following at the prompt to return to the root prompt:

`root` ↵

3 To configure LogViewer file parsing, perform the following steps.

i Press ↵ to enter command mode.

ii Enter the following at the root prompt:

`options` ↵

The following prompt is displayed:

```
log-options>
```

iii Enter y ↵ at the prompt to confirm the action.

iv To specify whether LogViewer parses the entire log file, enter the following at the prompt:

`parseAll` ↵

A confirmation prompt is displayed.

v To force LogViewer to reparse the current log file, enter the following at the prompt:

`reparse` ↵

vi If you are prompted to enable parsing of the entire log file, enter y ↵.

vii Enter the following at the prompt to return to the root prompt:

`root` ↵

Procedure 11-11 To specify plug-ins using the CLI

Perform this procedure to specify a plug-in for the current LogViewer CLI session.

1 Open the LogViewer CLI.

2 Press ↵ to enter command mode.

3 Enter the following at the root prompt:

`plugin` ↵

The following prompt is displayed:

```
log-plugin>
```

4 Enter the following at the prompt:

add ↵

LogViewer displays a list of the available plug-ins and the following prompt:

```
Which plugin would you like to specify? (name)
```

5 Enter the name of a plug-in from the list and press ↵.

6 You may be prompted for plug-in configuration information. Supply the information, as required.

Note — The currently available plug-ins and the associated configuration options are described in Procedure 11-8.

12 — Troubleshooting the 5620 SAM database

12.1 Database troubleshooting

Table 12-1 describes the problems associated with troubleshooting 5620 SAM database issues.

Table 12-1 5620 SAM database problems

Problem	Solution
Problem: Database corruption or failure	Procedure 12-1
Problem: The database is running out of disk space	Procedure 12-2
Problem: A short database backup interval is creating database performance issues	Procedure 12-3
Problem: A database restore fails and generates a No backup sets error	Procedure 12-4
Problem: Database redundancy failure	Procedure 12-5
Problem: Primary or standby database is down	Procedure 12-6
Problem: Need to verify that Oracle database and listener services are started	Procedure 12-7
Problem: Need to determine status or version of database or Oracle proxy	Procedure 12-8

12.2 Database troubleshooting procedures

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

Procedure 12-1 Problem: Database corruption or failure

You can restore a 5620 SAM database using a backup copy.

Note — Before you perform a database restore operation, you must shut down the databases and main servers in the 5620 SAM system. Contact Alcatel-Lucent technical support before you attempt to perform a database restore.

In a redundant 5620 SAM system, you must perform one or both of the following to regain database function and redundancy:

- Restore the primary database.
- Reinstantiate the standby database.

Both operations are required after a primary database failure. After a standby database failure, no restore operation is required, but you must reinstantiate the standby database to restore redundancy. You can use the 5620 SAM client GUI or a CLI script to reinstantiate a database.

Note 1 — In a redundant 5620 SAM system, you can restore a database backup only on a primary database station. To restore a database backup on a station other than the primary station, you must do the following on the station before you attempt the restore:

- Uninstall the 5620 SAM database, if it is installed.
- Install a primary database on the station.

Note 2 — In a redundant 5620 SAM system, you can reinstantiate a database only on a standby database station. To reinstantiate a database on a station other than the standby station, you must do the following on the station before you attempt the reinstantiation:

- Uninstall the 5620 SAM database, if it is installed.
- Install a standby database on the station.

See the *5620 SAM System Administrator Guide* for information about restoring a 5620 SAM database. See the 5620 SAM system redundancy chapter of the *5620 SAM User Guide* for information about 5620 SAM database reinstantiation.

Procedure 12-2 Problem: The database is running out of disk space

Sufficient database disk space is essential for efficient 5620 SAM database operation. You can also check whether your database backup schedule is adequate. Underscheduling backups while the database is in ARCHIVELOG mode creates numerous log files.

1. Verify that the database platform is adequately sized. The minimum platform requirements are available in the appropriate release notice or the *5620 SAM Planning Guide*, available from your Alcatel-Lucent technical-support representative.
2. Verify that the thresholds for disk space and archive logs are sufficient for your network, and determine how the disk space is being used. Contact your Alcatel-Lucent technical-support representative for more information.
3. Check the root database backup directory or partition to ensure that:
   - the size of the assigned disk space or slice is sufficient
   - the disk directory or slice is sufficient to hold the configured number of database backups
4. If the disk directory has many archived log files due to underscheduling of database backups, contact your Alcatel-Lucent technical-support representative for information about deleting archived log files.

5 Perform a database backup using the 5620 SAM client GUI or a C LI, as described in the *5620 SAM User Guide*.

6 Store the database backup in a secure location.

Procedure 12-3 Problem: A short database backup interval is creating database performance issues

Overscheduling the number of database backups can affect database performance, as the station uses excessive system resources to create the backups.

1 On a 5620 SAM client GUI, choose Administration→Database from the 5620 SAM main menu. The Database Manager form appears.

2 Click on the Backup tab.

3 Check the Backup Interval and Interval Unit parameters. For example, setting the Backup Interval parameter to 6 and setting the Interval Unit parameter to hour means a backup is performed every 6 hours, or four times a day.

This can cause performance issues, as station resources are used to create backups rather than to process requests.

4 Modify other parameters as required to improve performance.

5 Move the database backups to a secure location for storage or future use, according to your company policy.

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

Procedure 12-4 Problem: A database restore fails and generates a No backup sets error

Warning — Performing database modifications using Oracle database tools can cause irreparable harm to the database and your network management data, and can void your Alcatel-Lucent warranty or support agreement. Contact your Alcatel-Lucent technical-support representative for assistance with database troubleshooting.

Database backup sets expire based on a retention period. The default retention period is 365 days. After the retention period passes, the database backup sets are set to expired. You cannot restore databases from expired backup sets.

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

Procedure 12-5 Problem: Database redundancy failure

Warning — Performing database modifications using Oracle database tools can cause irreparable harm to the database and network management data, and can void your Alcatel-Lucent warranty or support agreement. Contact your Alcatel-Lucent technical-support representative for assistance with database troubleshooting.

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

- The primary and standby database directory structures and disk partition configurations are identical.
- The same OS version and 5620 SAM software release are installed on the primary and standby database stations.

2 Ensure that there are no network communication problems between the primary and standby database stations. See chapter 6 for more information.

Procedure 12-6 Problem: Primary or standby database is down

The status bar of the 5620 SAM client GUI indicates that the primary or standby database is down.

Warning — Performing database modifications using Oracle database tools can cause irreparable harm to the database and your network management data, and can void your Alcatel-Lucent warranty or support agreement. Contact your Alcatel-Lucent technical-support representative for assistance with database troubleshooting.

1 Verify the correct IP address and instance name of the database. From the 5620 SAM main menu, select Administration→Database to open the Database Manager. Verify the information in the Instance Name and DB Server fields.

2 Verify the network connectivity between the 5620 SAM primary server and the primary or standby database by ensuring that the primary server and the primary or standby database can ping each other. See chapter 6 for more information.

Procedure 12-7 Problem: Need to verify that Oracle database and listener services are started

Perform the following procedure to determine the status of the Oracle database and listener services, each of which starts automatically during system initialization.

1 Open a 5620 SAM GUI client.

2 View the status bar at the bottom of the GUI. The background of the database section of the status bar is yellow or red when there is a problem with a database service. The status bar text indicates the database service status.

Procedure 12-8 Problem: Need to determine status or version of database or Oracle proxy

Perform the following procedure to determine the status of the database or Oracle proxy, each of which starts automatically during system initialization.

1 Log in as the oracle management user on the database station.

2 Open a console window.

3 Navigate to the *installation_directory*/install/config/samdb directory

where *installation_directory* is the database installation location, typically /opt/5620sam/samdb

4 Enter the following command.

```
bash$ oracleproxy.sh option ↵
```

where *option* is one of the options in Table 12-2

Table 12-2 oracleproxy.* flag options

Flag option	Description
start	Starts the 5620 SAM Oracle proxy
no option, or help	Lists the available options
proxy_version	Displays Oracle proxy version information
proxy_status	Displays Oracle proxy status information
db_version	Displays 5620 SAM database version information
db_status	Displays 5620 SAM database status information

5 Review the command output.

The following sample shows the output of the proxy_status option.

```
Proxy is UP
```

The following sample shows the output of the db_version option.

```
5620 SAM Version 11.0 R1 - Built on Wed Mar 27 03:14:15 EST 2013
```

6 Close the console window.

13 — Troubleshooting 5620 SAM server issues

13.1 Troubleshooting 5620 SAM server issues procedures

Table 13-1 describes the problems associated with troubleshooting 5620 SAM server issues.

Table 13-1 5620 SAM server problems

Problem	Solution
Problem: Cannot start a 5620 SAM server, or unsure of 5620 SAM server status	Procedure 13-1
Problem: 5620 SAM server and database not communicating	Procedure 13-2
Problem: A 5620 SAM server starts up, and then quickly shuts down	Procedure 13-3
Problem: Client not receiving server heartbeat messages	Procedure 13-4
Problem: A 5620 SAM server cannot be reached over a network	Procedure 13-5
Problem: Excessive 5620 SAM server-to-client response time	Procedure 13-6
Problem: Unable to receive alarms on the 5620 SAM, or alarm performance is degraded	Procedure 13-7
Problem: All SNMP traps from managed devices are arriving at one 5620 SAM server, or no SNMP traps are arriving	Procedure 13-8
Problem: Cannot manage new devices	Procedure 13-9
Problem: Cannot discover more than one device, or device resynchronization fails	Procedure 13-10
Problem: Slow or failed resynchronization with network devices	Procedure 13-11
Problem: Statistics are rolling over too quickly	Procedure 13-12
Problem: Unable to receive alarms on the 5620 NM from the 5620 SAM	Procedure 13-13

13.2 Troubleshooting 5620 SAM server issues procedures

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

Note 1 — 5620 SAM server statistics collection is a useful troubleshooting tool for memory, alarm, and SNMP issues on a 5620 SAM main or auxiliary server. See the *5620 SAM Statistics Management Guide* for more information.

Note 2 — When no NE is associated with a 5620 SAM alarm, the alarm Site ID and Site Name properties are populated with the IP address and hostname, respectively, of the 5620 SAM main or auxiliary server that raised the alarm.

Procedure 13-1 Problem: Cannot start a 5620 SAM server, or unsure of 5620 SAM server status

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

- how long the server has been running
- the used and available memory
- the database connectivity status
- 5620 SAM license capacity

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

2 Open a console window.

3 To check the status of a 5620 SAM main server, perform the following steps.

i Enter the following at the CLI prompt:

***path*/nms/bin/nmsserver.bash appserver_status** ↵

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

General 5620 SAM server application status is displayed.

ii Enter the following at the CLI prompt:

***path*/nms/bin/nmsserver.bash nms_status** ↵

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

Detailed 5620 SAM server information is displayed.

iii To obtain more specific server status information, run the nmsserver script in step 3 using the appropriate option from Table 13-2 in place of the nms_status or appserver_status option.

Table 13-2 5620 SAM main-server startup script options

Option	Description
start	Starts the 5620 SAM main server in a non-interactive mode
stop	Stops the 5620 SAM main server
debug	Starts the 5620 SAM server in an interactive mode (1)
appserver_status	Returns information about the status of the 5620 SAM main server (both active and standby servers when the 5620 SAM is configured for redundancy)
appserver_version	Returns 5620 SAM software release information that includes the start time of the current 5620 SAM main server instance
nms_status	Returns the following information: • 5620 SAM standalone, primary, or standby server start time and running time • total used and available memory • database connectivity status • redundancy configuration and status • 5620 SAM license information • JVM memory-usage information • alarm forwarding information • basic auxiliary server information • number and status of current process threads
-v nms_status	Verbose version of the nms_status option that returns the following additional information: • ID and status of the current process threads • general JMS server information • currently connected JMS subscribers, by topic
-s nms_status	Short version of the nms_status option that returns the following information: • system information • IP address • database information • installation information
nms_info	Returns the following information from the 5620 SAM database: • number of managed devices by device type; for example, 7750 SR • number of MDA ports by type • number of equipped ports by type • number of services by type; for example, IES or VLL • number of access interfaces, connection termination points, and channels, by type • number of alarms, listed in order of severity • lists of enabled statistics, file, and accounting policies, including the counts and the polling frequency for different types of objects
nms_version	Returns 5620 SAM software release information
jvm_version	Returns version information about the currently running Java Virtual Machine environment
script_env	Returns main server script environment information
read_config	Rereads the nms-server.xml server configuration file while the server is running in order to put configuration file updates into effect
force_restart	Forces the 5620 SAM main server to restart

(1 of 2)

Option	Description
force_stop	Forces the 5620 SAM main server to stop
passwd <*username*> <*current*> <*new*> where *username* is the database username, for example, samuser *current* is the current password *new* is the new password	Changes the database user password
read_metrics_config	Reads the server metrics configuration file
import_license	Imports a new license zip file for the server
threaddump	Prints a thread dump for every SAM java process running on the station
webstart	Starts the web server
webstop	Stops the web server
webstatus	Prints web server status
webforce_restart	Forces the web server to restart
webforce_stop	Forces the web server to stop and not restart
jmsstart	Starts the JMS server in interactive mode
jmsstop	Stops the JMS server
jmsstatus	Returns information that includes the following: • general JMS server information • currently connected JMS subscribers, by topic
jmsread_config	Rereads the JMS server configuration file while the JMS server is running
jmsforce_restart	Forces the JMS server to restart
jmsforce_stop	Forces the JMS server to stop
jmsjvm_version	Returns version information about the currently running Java Virtual Machine environment
jmsappserver_status	Returns the JMS server status
jmsscript_env	Returns the JMS script environment
no keyword, help, or ?	Lists the available command options

(2 of 2)

Note
(1) The server shuts down if the console is closed or if CTRL-C is pressed.

4 To check the status of a 5620 SAM auxiliary server, perform the following steps.

i Enter the following at the CLI prompt:

***path*/nms/bin/auxnmsserver.bash aux_status** ↵

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

The general 5620 SAM server application status is displayed.

ii Enter the following at the CLI prompt:

***path*/nms/bin/auxnmsserver.bash auxappserver_status** ↵

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

Detailed 5620 SAM server information is displayed.

iii To obtain more specific server status information, run the nmsserver script using the appropriate option from Table 13-3 in place of the aux_status or appserver_status option.

Table 13-3 5620 SAM auxiliary-server startup script options

Option	Description
auxappserver_status	Returns information about the operational status of the auxiliary server
auxdebug	Starts the auxiliary server in interactive mode
auxforce_restart	Forces the auxiliary server to restart
auxforce_stop	Forces the auxiliary server to stop
auxjvm_version	Returns the auxiliary server JVM version
auxread_config	Directs the auxiliary server to read and apply the settings in the general configuration file
auxread_metrics_config	Directs the auxiliary server to read and apply the settings in the metrics configuration file
auxscript_env	Returns auxiliary server script environment information
auxstart	Starts the 5620 SAM auxiliary server
auxstatus	Returns information about the auxiliary server that includes the following: • IP address • port number • database connections • installed server software release ID
auxstop	Stops the 5620 SAM auxiliary server
aux_version	Returns auxiliary server software release information
auxthreaddump	Returns a thread dump for every auxiliary server process currently running on the station
auxhelp, *no keyword*, or ?	Lists the available command options

5 Review and record the displayed information for Alcatel-Lucent technical-support, if required.

6 Close the console window.

7 View the 5620 SAM server logs for error messages using the 5620 SAM LogViewer GUI application, as described in chapter 11.

8 Report the error messages that you find to an Alcatel-Lucent technical support representative.

Procedure 13-2 Problem: 5620 SAM server and database not communicating

Perform this procedure when a 5620 SAM server cannot connect to a 5620 SAM database.

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

2 Ensure that the ports specified at installation time are available and not being blocked by firewalls. See chapter 6 for more information.

3 Perform the following troubleshooting activities for the primary database, as described in Procedure 12-6.

- Verify the correct IP address and instance name of the database.
- Verify that the database instance is running.
- Verify that the database is running in the correct mode.

See the *5620 SAM Planning Guide* for more information about the ports that must be available for the 5620 SAM to function. If the problem persists, collect the logs identified in Procedure 10-1 and contact your Alcatel-Lucent support representative.

Procedure 13-3 Problem: A 5620 SAM server starts up, and then quickly shuts down

When a server starts then stops, collect the logs identified in Procedure 10-1 and contact your Alcatel-Lucent support representative.

Procedure 13-4 Problem: Client not receiving server heartbeat messages

Perform this procedure when a 5620 SAM client is not receiving heartbeat messages.

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

2 Verify that the 5620 SAM server and client clocks are synchronized. To set the date and time for 5620 SAM server and client clocks, see the *5620 SAM System Administrator Guide* for more information.

Procedure 13-5 Problem: A 5620 SAM server cannot be reached over a network

Perform this procedure to check the IP connectivity between a 5620 SAM client and main server using ping commands. When the ping commands indicate that IP communication is active but there are still IP reachability issues, the problem could be poor LAN performance.

1 Perform a ping test to measure reachability, as described in Procedure 6-2.

2 On a RHEL or Solaris station, if you cannot ping the 5620 SAM server, make sure that the hostname of the server is in the /etc/hosts file. Perform the following steps.

i Change to the /etc directory by typing:

cd /etc ↵

ii Open the hosts file with a text editor, for example, vi.

iii Add the hostname 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 13-6 Problem: Excessive 5620 SAM server-to-client response time

As the number of managed devices grows and as more GUI or OSS clients are brought online, the processing load on the 5620 SAM system increases. For optimum 5620 SAM performance, you must ensure that the 5620 SAM configuration meets the requirements in the *5620 SAM Planning Guide* as your network expands.

You can do the following to increase the available 5620 SAM server network management resources:

- Deploy the 5620 SAM system in a distributed configuration.
- Deploy the 5620 SAM system in a redundant configuration.
- Deploy 5620 SAM auxiliary servers.
- Reallocate the 5620 SAM server resources that are assigned to groups of managed devices.

See the *5620 SAM User Guide*, *5620 SAM System Architecture Guide*, and the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about a particular option. Contact Alcatel-Lucent support for reconfiguration assistance.

Perform this procedure to check the following:

- 5620 SAM auxiliary server status

  System performance may degrade if the number of available Preferred and Reserved auxiliary servers drops below the number of configured Preferred auxiliary servers.
- 5620 SAM main server status

  Alarms raised against the 5620 SAM main server may provide information about the performance degradation.

Caution — Only Alcatel-Lucent support staff are qualified to assess and reconfigure a 5620 SAM deployment.

1 Open a 5620 SAM client GUI.

2 Choose Administration→System Information. The System Information form opens.

3 Click on the Faults tab to view auxiliary server and general 5620 SAM system alarm information, if required.

4 If your 5620 SAM deployment includes one or more auxiliary servers, perform the following steps to check the status of each auxiliary server.

i Click on the Auxiliary Servers tab.

ii Review the list of auxiliary servers.

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

iv Review the information, which includes:

- the auxiliary server IP address
- the auxiliary server hostname
- the auxiliary server port number
- the auxiliary server type (Reserved or Preferred)
- the auxiliary server status (Unknown, Down, Up, or Unused)

v If the auxiliary server status is Down, perform Procedure 13-1 on the auxiliary server.

vi If the auxiliary server status is Unknown, perform Procedure 13-11 to check the connectivity between the managed network and the main and auxiliary servers.

5 Close the System Information form.

Procedure 13-7 Problem: Unable to receive alarms on the 5620 SAM, or alarm performance is degraded

By default, the system begins purging alarms when the outstanding alarm count reaches 50 000, unless historical alarm record logging and purging alarm policies are configured to keep the outstanding alarm count below that level.

Caution — Exceeding the alarm limit configured in the nms-server.xml file may cause system performance problems.

1 Check the status bar of the 5620 SAM client GUI status bar for indications that the maximum number of alarms for the system is reached.

2 If required, clear outstanding alarms or delete them to the alarm history record log, as described in the *5620 SAM User Guide*.

3 If the 5620 SAM system includes one or more auxiliary servers, perform Procedure 13-6 to ensure that system performance is not degraded because of auxiliary-server unavailability.

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

Procedure 13-8 Problem: All SNMP traps from managed devices are arriving at one 5620 SAM server, or no SNMP traps are arriving

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

- Enable key SNMP parameters on the devices before managing them.
- Ensure that a unique trapLogId is specified for each router to communicate with the 5620 SAM. If the trapLogId is used by other applications or by another 5620 SAM, traps may be misdirected or directed to only one machine.

Note — You must have sufficient user permissions, for example, admin permissions, to configure SNMP on a device.

1 See the commissioning chapter of the *5620 SAM User Guide* for more information about configuring devices for 5620 SAM management, including enabling the SNMP engine and defining at least one SNMP community.

2 Configure SNMP on the device using CLI.

Procedure 13-9 Problem: Cannot manage new devices

The possible causes are:

- The number of managed devices or MDAs exceeds the licensed quantity.
- 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 licensed MDA limit is exceeded.

Caution — Do not modify other nms-server.xml parameters. Modifying the file can seriously affect network management and performance of the 5620 SAM.

1 Check the license key status.

i The 5620 SAM generates an alarm when a license limit is exceeded or nearly exceeded. View the dynamic alarm list in the 5620 SAM client GUI, or the JMS real-time alarm feed from a 5620 SAM OSS client application for alarms related to nearing or exceeding a license limit.

ii Choose Help→5620 SAM License Information from the 5620 SAM main menu. The 5620 SAM License (Edit) form opens.

iii Click on the Devices and Quantities Licensed tab.

iv View the information to ensure that the required Remaining quantity is not equal to zero.

Note — If you have a new license that supports a greater number of managed objects, you can dynamically update the license without restarting the main server. See the *5620 SAM User Guide* for information about updating a 5620 SAM license.

v Close the 5620 SAM License (Edit) form.

2 Ensure that the new devices are configured to send SNMP packets of up to 9216 bytes. Check the MTU size, as described in Procedure 6-4.

Procedure 13-10 Problem: Cannot discover more than one device, or device resynchronization fails

Consider the following:

- When using SNMPv3 encryption, the engine ID of the managed device must be unique. As well, SNMP issues may result in Polling Problem alarms. Otherwise, the following issues may occur:
  - unreliable or slow discovery of network devices
  - resynchronization during scheduled polling fails
  - slow communication and synchronization times
  - polling fails completely
- When 5620 SAM resynchronizes some functions on an NE, for example, BGP configurations for the 7750 SR, the SNMP packets may be broken into two or more smaller packets, when the maximum PDU size of 9216 bytes is exceeded.
- Each MIB entry policy has its own polling interval. When there is insufficient time in a polling interval for a resynchronization to occur, the interval may need to be changed to ensure proper resynchronization.

1 For resynchronization issues that may be caused due to insufficient MIB polling intervals.

2 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens with the General tab selected.

3 Ensure that the Polling Admin State is Up.

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

4 Check the MIB polling intervals for different managed devices, as required, by clicking on the MIB Entry Policies tab. A list of MIBs appears, organized by managed device type.

i Select a MIB in the list and click on the Properties button.

ii Configure the Polling Interval parameter to ensure that sufficient time is configured for the polling to occur.

iii Configure the Administrative State of polling for the MIB entry, if required.

iv Click on the OK button to save the changes and close the form, or the Cancel button to close the form without saving changes, as required.

Procedure 13-11 Problem: Slow or failed resynchronization with network devices

When 5620 SAM performance is slow, especially when performing network device resynchronizations, SNMP and IP performance along the in-band or out-of-band interfaces between the network device and the 5620 SAM server may be the problem. Check the following:

- configuration of the LAN switch port and the 5620 SAM station port match
- configuration of the LAN switch port and the network device management ports match
- mediation policy SNMP timeout and retry values are sufficient to allow the transfer of data between network devices and the 5620 SAM

1 Ensure that port configurations are compatible for the 5620 SAM server, the network device management ports, and the LAN switch. This is normally done by configuring auto-negotiation between the platforms, but your network may require more specific configuration.

2 Check whether all data is being transferred between the network device in-band management port and the 5620 SAM server.

i Open a Telnet or SSH session to the device from the 5620 SAM.

ii Check statistics on the in-band management port of the device:

```
# monitor port 1/2/3
```

Check the output for the following.

- errors that may indicate a communication problem with the a LAN switch.
- Over each time interval, is the number of input and output packets constant? This may indicate intermittent traffic.
- Are there more input packets or octets being transferred than output packets or octets? This may indicate a unidirectional traffic problem.

The types of error messages displayed determine the action to take.

- For failure errors, consider increasing the SNMP timeout value
- For collision errors, consider increasing the SNMP retry value

iii Check the mediation policy for the device using the 5620 SAM client GUI. Check the SNMP timeout and retry value for the mediation policy.

If the output of step ii indicates failures, consider increasing the default SNMP timeout value and perform step ii again.

When the output of step ii indicates frequent collisions, consider increasing the default SNMP number of retries value, then retest to see if resynchronizations are more reliable. Increasing the number of retries increases the likelihood that an SNMP packet is not dropped due to collisions.

You can check SNMP timeout and retry values from the Administration→Mediation menu. Click on the Mediation Security tab.

Caution — When LAN performance is poor, increasing timeout values may mask an underlying problem. Increasing the SNMP timeout value in an environment where collisions are frequent reduces performance. Timeout values should be based on typical network response times

Check LAN communication issues, as specified in chapter 6. If problems persist, collect the logs as specified in Procedure 10-1 and contact your Alcatel-Lucent support representative.

Procedure 13-12 Problem: Statistics are rolling over too quickly

Statistics database tables roll over, or lose statistics during an interval, if the tables fill before all statistics are collected or the next collection interval starts. To ensure sufficient statistics collection, consider the following:

- the statistics table size, depending on the configuration specified in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*
- the number of statistics collected, the number of objects with statistics collection enabled, and the frequency of statistics collection, as specified in the *5620 SAM User Guide*

- the OSS application requests data from the statistics tables less frequently than the configured roll over interval
- FTP must be enabled on the managed device in order for the 5620 SAM to retrieve statistics.

Alcatel-Lucent recommends that statistics collection planning includes the following considerations to prevent the loss of statistics data.

- measure the rate of statistics collection over a sufficient time interval
- determine the appropriate collection interval and statistics database table size based on individual network configurations
- ensure that the polling interval is sufficient for polled statistics

Procedure 13-13 Problem: Unable to receive alarms on the 5620 NM from the 5620 SAM

Check that the 5620 NM AS tool is properly configured to receive 5620 SAM alarms.

1 Ensure that the integration software is properly configured, as described in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

2 Configure the param.cfg file on the 5620 NM to ensure that alarms are forwarded from the 5620 SAM to the 5620 NM AS tool:

3 Open a command tool on the 5620 NM.

4 Navigate to the AS IM directory on the 5620 NM by typing:

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

5 Open the param.cfg file.

6 Set the NSP_USE_NSP parameter to True.

7 Ensure that the following param.cfg file parameters are configured to True:

- DROP_FREE_ALARMS
- CORBA_SERVER_DISCOVERY
- UNMANAGE_ON_TERMINATION

8 Save the changes and close the file.

14 — Troubleshooting 5620 SAM clients

14.1 Troubleshooting 5620 SAM client GUIs and client OSS applications

Table 14-1 describes the problems associated with troubleshooting 5620 SAM client GUIs and client OSS applications.

Table 14-1 5620 SAM client GUIs and client OSS applications problems

Problem	Solution
Troubleshooting common client application problem	
Problem: Cannot start 5620 SAM client, or error message during client startup	Procedure 14-1
Problem: 5620 SAM client unable to communicate with 5620 SAM server	Procedure 14-2
Problem: Delayed server response to client activity	Procedure 14-3
Problem: Cannot view 5620 SAM alarms using 5620 NM client	Procedure 14-4
Problem: Unable to print from RHEL or Solaris client	Procedure 14-5
Problem: Cannot place newly discovered device in managed state	Procedure 14-6
Problem: I performed an action, such as saving a configuration, but I cannot see any results	Procedure 14-7
Problem: Device configuration backup not occurring	Procedure 14-8
Troubleshooting client GUI issues	
Problem: 5620 SAM client GUI shuts down regularly	Procedure 14-9
Problem: Configuration change not displayed on 5620 SAM client GUI	Procedure 14-10
Problem: List or search function takes too long to complete	Procedure 14-11
Problem: Cannot select certain menu options or cannot save certain configurations	Procedure 14-12
Problem: Cannot clear alarms using 5620 SAM client GUI	Procedure 14-13
Problem: The 5620 SAM client GUI does not display NE user accounts created, modified, or deleted using the CLI	Procedure 14-14

14.2 Troubleshooting common client application problem procedures

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

Procedure 14-1 Problem: Cannot start 5620 SAM client, or error message during client startup

Check the following:

- the 5620 SAM client and server have the same software versions and compatible patch sets
- the login name and password of the user are correct

- there are no OS errors
- a local firewall is running on the client station

1 If the 5620 SAM client is installed on RHEL or Solaris and you receive a "Cannot execute" message when you try to run the client, the client executable file permission may have been reset by an event such as an auto-client update failure. Perform the following steps to correct this.

   i Log in as root, or as the user that installed the 5620 SAM client, on the client station.

   ii Open a console window.

   iii Enter the following at the CLI prompt to set the execute-permission flag on the client executable file:

   # **chmod +x *path*/nms/bin/nmsclient.bash**

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

2 Review the login pop-up messages that appear when a client GUI attempts to connect to a server. Messages that state things like the server is starting or the server is not running indicate the type of communication problem.

3 To check that the login name and the password of the user are correct, modify the login and password as 5620 SAM admin and have the user attempt to log in.

   i Start the 5620 SAM client as the admin user.

   ii Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The Security Management (Edit) form appears with the General tab displayed.

   iii Click on the Users tab.

   iv Configure the list filter criteria and click on the Search button. A list of users is displayed.

   v Select a user.

   vi Click on the Properties button. The User (Edit) form appears.

   vii Enter a new password for the User Password parameter.

   viii Confirm the password for the Confirm Password parameter.

   ix Click on the Apply button to save the changes.

   x Have the user attempt to start a 5620 SAM client and log in.

4 To check that the 5620 SAM server is up and to view additional server configuration information, perform the following steps.

   i Log on to the 5620 SAM server station as the samadmin user.

   ii Open a console window.

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

iv Enter the following at the CLI prompt:

`./nmsserver.bash appserver_status` ↵

Server status and configuration information are displayed.

v To check additional server status conditions, perform Procedure 13-1.

5 Check the client GUI login error message.

When a firewall is running locally on the client station, a login error message may appear indicating that the server is not available. Ensure that a local firewall is not preventing a connection to the server, and that the 5620 SAM server IP address is in the client host-lookup file.

Procedure 14-2 Problem: 5620 SAM client unable to communicate with 5620 SAM server

Before you proceed, ensure that the following conditions are present.

- The 5620 SAM client points to the correct IP address and port of the server.
- The problem is not a network management domain LAN issue. See chapter 6 for more information.
- Firewalls between the 5620 SAM clients and the server are correctly configured

1 To check that the 5620 SAM client points to the correct IP address and port of the server, open the nms-client.xml file using a text editor. The default file location is *installation_directory*/nms/config.

where *installation_directory* is the directory in which the 5620 SAM client software is installed, for example, /opt/5620sam/client

2 Verify the IP address of the server as specified by the ejbServerHost parameter.

3 Verify the server port as specified by the ejbServerPort parameter.

4 Modify the IP address and port values, if required.

5 Save the file, if required.

6 Perform Procedure 13-1 to check the server status. A client cannot connect to a 5620 SAM server that is not started.

7 If the server is started, compare the firewall and network configuration guidelines in the *5620 SAM Planning Guide* to with your network configuration to ensure that it complies with the guidelines.

8 Contact your Alcatel-Lucent support representative if the problem persists.

Procedure 14-3 Problem: Delayed server response to client activity

Possible causes are:

- a congested LAN
- improperly sized platforms

Using the netstat command on the client may help troubleshoot network throughput problems. When an Ethernet LAN is highly congested, the actual throughput slows down. This is caused by packets colliding on the LAN as multiple machines begin to transmit at approximately the same time, for example, when multiple 5620 SAM client GUIs or OSS applications are performing simultaneous tasks.

1 Client GUIs may respond more slowly than normal during resynchronizations of managed devices. Repeat the client GUI action when the resynchronization is complete.

2 Check for LAN throughput issues.

i Open a shell console window.

ii Enter the following at the console prompt to display local network-interface transmission data over a period of time:

```
# netstat -i s ↵
```

where *s* is the time, in seconds, over which you want to collect data. Alcatel-Lucent recommends that you start with 50 s

iii Review the output. The following is sample netstat output:

```
netstat -i 5

 input   le0       output           input  (Total)    output

packets errs  packets errs  colls packets errs  packets errs
colls

6428555 41    541360  80    49998 6454787 41    567592  80
49998

22      0     0       0     0     22      0     0       0     0

71      0     7       0     3     71      0     7       0     3
```

This sample displays the number of input and output packets, errors and collisions on the le0 interface. One column displays the totals for all interfaces. This sample only has one interface, so both sets of columns display the same data.

Calculate the number of collisions as a percentage of the number of output packets. For example, according to the last line of output, there were three collisions and seven output packets resulting in a 42% rate.

This number is high, but the time in which the sampling was obtained (5 s), was low. Change the sample rate to, for example, 50 s for an accurate sampling of the network throughput.

When collisions are between 2% and 5%, congestion on the interface is within the normal operating range.

In a typical network, when collisions are greater than 5%, you may have a serious congestion problem on the interface. Review your LAN topology and design to reduce the number of network bottlenecks.

iv To stop the command, press CTRL-C.

3 Check that the client platform is appropriately sized. See the *5620 SAM Planning Guide* for more information.

Procedure 14-4 Problem: Cannot view 5620 SAM alarms using 5620 NM client

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

1 Open a command tool on the 5620 NM client station.

2 Navigate to the AS tool IM directory by typing:

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

3 Open the param.cfg file.

4 Ensure the NSP_USE_NSP and CORBA_SERVER_DISCOVERY parameters are set to True.

5 Save the changes and close the file.

6 When the filters for CORBA are set to True, ensure the CORBA filter files are set correctly. Navigate to the AS tool IM configuration directory by typing:

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

7 Ensure the following filters are set in the ASIMconfig or ASIMFilter files:

```
CORBA_ROOT_NAME_FILTER="*/*/AlarmSynchronizer*";

CORBA_ROOT_NAME_FILTER="*/*/EventChannelFactory*";

CORBA_ROOT_NAME_FILTER="*/*/X733EventChannel*";
```

8 Save the changes and close the file.

Procedure 14-5 Problem: Unable to print from RHEL or Solaris 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.

See the OS documentation and the printer documentation for more information about printer configuration.

If you are using a printer server, ensure that the printer is listed in the /etc/hosts file

Table 14-2 lists some common printer problems.

Table 14-2 Troubleshooting RHEL or Solaris printer problems

Problem	Probable cause	Solution
A new user cannot print	No entry for that printer in the user account .cshrc file	Add printer entry to .cshrc file
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	User logout and subsequent login
A user cannot delete a printer	There are print jobs in the queue for that printer	Delete queued print jobs using lprm command
The client cannot print	The printer was not added to the list of available printers	Add printer to printer list using admintool

1 On the station, log in as the user that has 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 station 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 14-6 Problem: Cannot place newly discovered device in managed state

Possible causes are:

- the number of managed cards (MDAs) exceeds the 5620 SAM server license
- another application using a port required by the 5620 SAM server
- resychnronization problems between the managed network and the 5620 SAM

See Procedure 13-9 for more information.

Procedure 14-7 Problem: I performed an action, such as saving a configuration, but I cannot see any results

Possible causes are:

- Failed SNMP communication between the server and managed device. See Procedure 13-8 for more information.
- Failed deployment of the configuration request.

1 For the 5620 SAM client, perform the following:

i Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu.

The Deployment form opens with the Incomplete Deployments tab displayed. Incomplete deployments are listed, and deployer, tag, state and other information is displayed. The possible states for a deployment are:

- Deployed
- Not Deployed
- Pending
- Failed — Resource Unavailable. Failure occurred because one of the resources required to apply the configuration is not present in the 5620 SAM database
- Failed — Configuration. Failure occurred because the configuration could not be applied to the specified objects
- Failed — Partial. Failure occurred at deployment and some of the configuration can been sent to the network
- Failed — Internal Error. Failure a occurred due to general error conditions. Code is intended as a catch-all code for all other possible errors
- Cancelled
- Postponed

You can also suspend or resume deployment retries by clicking on the Suspend Retries or Resume Retries button. You can clear a deployment by clicking on the Clear button. When you clear a deployer, no further attempt is made to reconcile the network device status with the 5620 SAM database. Affected objects should be resynchronized.

If a deployment is not sent to a managed device, the intended configuration change is not made on the device.

ii Choose a failed deployment and click on the Properties button to view additional information. The deployment properties form opens.

2 When a deployment fails and you receive a deployment alarm, check the following:

i Using CLI, check on the device whether the deployment change is on the device.

ii If the change is on the device, the deployment alarm was likely raised because the configuration already exists on the device. Clear the failed deployment and resynchronize the device with the 5620 SAM.

If the change is not on the device, collect the information from the deployment properties form and contact your Alcatel-Lucent support representative.

3 For client OSS applications, perform the following:

Note — These steps describe how to troubleshoot asynchronous deployment requests only. Alcatel-Lucent recommends that deployment requests be made in asynchronous mode.

i Browse real-time alarms received via JMS. An alarm denoting a deployment failure contains the following text:

```
Attribute: alarmClassTag Value: generic.DeploymentFailure
```

The alarm also contains additional information, including the object affected by the alarm and the severity of the alarm. See the *5620 SAM XML OSS Interface Developer Guide* for more information.

ii Find the following text in the alarm:

```
Attribute: requestID=requestID
```

The parameter specifies the request id sent with the original request. The request id should be unique per request.

iii Determine the original request using the request id.

iv Troubleshoot the original request. If there are problems with the original request, clear the deployer, fix the request, and send the new request. See the *5620 SAM XML OSS Interface Developer Guide* for more information.

v If there are no problems with the original request, the failure may be caused by a network communication or device failure, or by packet collisions caused by conflicting configurations. You can:

- resend the request
- troubleshoot your network or device

Procedure 14-8 Problem: Device configuration backup not occurring

1. Use the 5620 SAM client to check the device database backup settings. Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens with the Backup/Restore Policy tab displayed.
2. Click on the Backup/Restore Status tab. The managed devices are listed and backup and restore status information is displayed.
3. Select the device and click on the Properties button. The NE Backup/Restore Status form opens with the General tab displayed.
4. View the information in the Backup Status panel. A Backup State other than Successful may indicate a communication problem or a backup policy configuration error.
5. Ensure that the device configuration file and the associated index file are saved on the device and available for backup. Click on the Configuration Saves tab, and ensure that the Config Save State indicator reads Success.

   See the appropriate device OS documentation for more information.
6. Click on the Backups tab to view a list of backup operations that are currently in progress. A backup operation disappears from the list after it completes.
7. Click on the Faults tab to view additional troubleshooting information.
8. Close the NE Backup/Restore Status form.The Backup/Restore form is displayed.
9. Use the information obtained from the NE Backup/Restore Status form to check the backup policy configuration, if required. Click on the Backup/Restore Policy tab.
10. Select the backup policy for the device and click on the Properties button. The Backup Policy (Edit) form opens with the General tab displayed.
11. Ensure that the policy is assigned to the device.
    - **i** Click on the Backup/Restore Policy Assignment tab.
    - **ii** If required, configure a filter and click on the OK button.
    - **iii** Move the device to the Assigned Sites list if it is not there by selecting the site from the Unassigned Sites list and clicking on the right-arrow button.
    - **iv** Click on the Apply button to save changes, as required.
12. Click on the General tab.
13. Verify the parameter settings and modify, if required.
14. Click on the OK button to save the changes and close the form.

14.3 Troubleshooting client GUI issues procedures

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

Procedure 14-9 Problem: 5620 SAM client GUI shuts down regularly

The 5620 SAM client GUI automatically shuts down under the following conditions:

- no activity on the GUI for a specified amount of time
- no communication between the GUI and the server for a specified amount of time.
- when there is an communication error that causes problems between the server and the client

Note — Changing the OS clock setting on the server station can cause communication problems on the client. If the server clock setting changes significantly, the clients must log off and the server must be restarted. Alcatel-Lucent recommends that the server OS clock be tied to a synchronous timing source to eliminate time shifts that may lead to polling and communication problems.

1 Disable the GUI activity check, if required. Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The Security Management (Edit) form appears with the General tab selected.

2 Set the Client Timeout (minutes) parameter to 0 to disable the GUI inactivity check. Alternately, you can configure a higher value for the parameter, to increase the time that must pass before the client GUI is shut down due to inactivity.

3 Click on the Apply button and close the form.

Procedure 14-10 Problem: Configuration change not displayed on 5620 SAM client GUI

The 5620 SAM supports the configuration of complex objects, for example, services, using configuration forms or templates. Additional configuration forms and steps may be contained by 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. Alternatively, when you use service templates, parent templates for site configuration must also be configured.

Objects configured in contained configuration forms are not saved until the parent configuration form is saved. For example, when you configure a VLL service, sites or L2 interfaces that you configure are not saved during service creation until the parent configuration form is saved. You cannot view new objects or new object configurations in other parts of the GUI, such as the navigation tree, until the service is saved.

The 5620 SAM displays a dialog box to indicate that configured objects in a configuration form are not saved until the parent configuration forms are saved.

Procedure 14-11 Problem: List or search function takes too long to complete

You can perform simple listings or complex searches using the Manage menu on the 5620 SAM main menu to query the database for information about services, customers, and other managed entities.

Depending on the type of information and the number of entries returned, a list or search operation may take considerable time to complete. As a general rule, Alcatel-Lucent recommends that you use filters to restrict the number of items in a list or search operation to 10 000 or fewer.

See the *5620 SAM User Guide* for information about the 5620 SAM client GUI list and search functionality. See the *5620 SAM Planning Guide* for information about 5620 SAM scalability and system capacity guidelines.

Procedure 14-12 Problem: Cannot select certain menu options or cannot save certain configurations

The 5620 SAM allows the administrator to restrict access to parts of the GUI, or restrict the ability of a user to configure objects or save configurations. Check with your administrator to determine your permissions and scope of command.

When an administrator changes user or user group permissions from the 5620 SAM security menus, the changes take effect immediately and determine the actions that a user can perform from the client GUI.

As well, the 5620 SAM license must enable the appropriate software module to perform a certain function. See Procedure 13-9 for more information about viewing license information to determine which modules are installed.

Procedure 14-13 Problem: Cannot clear alarms using 5620 SAM client GUI

If you cannot clear alarms, there may be an underlying database issue. Collect the logs outlined in Procedure 10-1 and contact your Alcatel-Lucent support representative.

Procedure 14-14 Problem: The 5620 SAM client GUI does not display NE user accounts created, modified, or deleted using the CLI

When an NE user account is created, modified, or deleted using the CLI, the 5620 SAM client GUI does not update the user list in the NE User Profiles form. For increased security, the NE does not send a trap for changes made to NE user accounts. You can update the 5620 SAM with the NE user account changes by resynchronizing the NE.

1 Choose Equipment from the 5620 SAM navigation tree drop-down menu.

2 Navigate to the NE. The path is Network→NE.

3 Right-click on the NE and choose Resync.

The Resync menu option specifies that SNMP MIB and CLI information bases are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.

Customer documentation and product support

Customer documentation

Customer Documentation Welcome Page

Technical Support

http://support.alcatel-lucent.com

Documentation feedback

documentation.feedback@alcatel-lucent.com

www.alcatel-lucent.com