Alcatel-Lucent 5620

SERVICE AWARE MANAGER

INTEGRATION 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

Integration configuration

Integration configuration

1 — 5620 SAM integration overview

1.1 Introduction

The *5620 SAM Integration Guide* describes several configurations that enable the 5620 SAM to integrate with other systems. Integration has different forms, depending on the components involved and the type of integration required. For example, a horizontal integration protocol is often used to provide east-west integration between products.

1.2 Integration overview

The *5620 SAM Integration Guide* contains information about integrating the 5620 SAM with third-party and Alcatel-Lucent systems to enable additional functions. The 5620 SAM can also be integrated with systems that augment the behavior of previously integrated systems, such as Single Sign On and CFMA.

Integration with other systems

A 5620 SAM system operates interactively with other systems to provide additional functions and greater ease of use. Depending on the type of integration, the interface of one system can be used to perform functions on, or retrieve information from, the other system.

See chapter 2 for more information.

Integration with Single Sign On

Single Sign On (SSO) technology enables an operator to access all resources in a domain after having entered the user credentials only once.

See chapter 3 for more information.

Integration with CFMA

The SAM-CFMA adapter for CFMA translates 5620 SAM alarms into CFMA alarms. Using CFMA as a fault manager, the adapter is used to aggregate 5620 SAM alarms within another NM.

The adapter connects to the 5620 SAM using a 5620 SAM-O JMS connection. The adapter software is in the integration/samcfmadapter directory of the 5620 SAM installation software file set.

See chapter 4 for more information.

Integration with Chronos SyncWatch

The Chronos SyncWatch Probe provides a system for synchronization testing and monitoring for network management purposes. The NetSMART Server provides remote management of multiple SyncWatch Probes. It collects data that can be used to alert users to potential synchronization problems.

The 5620 SAM provides integration support for both the SyncWatch Probe and the NetSMART Server components. The 5620 SAM provides basic network element management support at the GNE level for the probe, as well as a fault management framework to manage synchronization-related alarms.

See chapter 5 for more information.

2 — 5620 SAM integration with other systems

2.1 5620 SAM integration overview

You can integrate the 5620 SAM with a variety of other systems. Integration allows the 5620 SAM to provide a broader range of management functions from a single GUI. This chapter describes the configuration of different integration scenarios.

2.2 5620 SAM and 5650 CPAM integration

The 5650 CPAM provides real-time control-plane IGP and BGP topology capture, inspection, visualization, and troubleshooting. The 5650 CPAM can be integrated with the 5620 SAM, or installed as an independent system. Integration allows the 5650 CPAM to associate routing information with 5620 SAM network routes, service tunnels, LSPs, edge-to-edge service traffic paths, and OAM tests.

When the 5650 CPAM software is enabled on a 5620 SAM system, the 5650 CPAM functions are available from the 5620 SAM main menu. See the *5650 CPAM User Guide* for more information.

The 5650 CPAM provides a tight eastbound and westbound integration with the 5620 SAM. This integration allows for a real-time view of the network including routing topology and associated configurations whether performed on the GUI, OSS interface, or by CLI. The 5650 CPAM can leverage 5620 SAM redundancy and offer tight navigation between protocol maps and 5620 SAM-managed objects, such as protocol links. In addition, the 5620 SAM GUI supports the management of the 7701 CPAA platform.

When the 5650 CPAM and the 5620 SAM share the same database, the 5650 CPAM can access objects managed by 5620 SAM and display them on the 5650 CPAM topology views. Without integration with the 5620 SAM, the following functions are not available:

- service, LSP, multicast, and OAM highlights
- historical LSP active paths
- LDP and RSVP interface display on the MPLS view
- auto-OAM function that uses STM test policies for IP and LSP path monitors

The 5650 CPAM route controller, or server, communicates with GUI and OSS clients using the same API as the 5620 SAM. When the 5650 CPAM route controller is integrated with a 5620 SAM, the 5620 SAM and 5650 CPAM releases must be compatible. In addition, the 5650 CPAM route controller can run independently with one or multiple 5620 SAM servers.

5650 CPAM deployment

The 5650 CPAM system requirements are the same as the 5620 SAM main server requirements. The *5620 SAM Planning Guide* contains information such as platform specifications, scaling guidelines, and network requirements. The *5620 SAM | 5650 CPAM Installation and Upgrade Guide* contains deployment information such as the following:

- deployment considerations
- integration with the 5620 SAM during main server installation or upgrade

- independent installation and upgrade as a standalone or redundant system
- uninstallation

5650 CPAM integration with the 5620 SAM requires a license file in compressed format. Alcatel-Lucent generates a 5650 CPAM license file based on the system ID of the station that is to host the software. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about how to obtain the system ID of a station.

Note 1 — The Alcatel-Lucent Software License Manager, or ASLM, accepts only the UUID of a station as the system ID.

Note 2 — The license files of 5620 SAM and 5650 CPAM servers that share a station must be generated using the same system ID.

You can specify the inclusion of an integrated 5650 CPAM server during a 5620 SAM main server installation or upgrade. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information.

You can integrate the 5650 CPAM with an existing 5620 SAM main server by importing the 5650 CPAM license file to the main server configuration. The 5650 CPAM client GUI functions are not enabled until you restart the client. See Procedure 2-1 for more information.

5650 CPAM menus

The following 5650 CPAM menu items do not display, or are disabled, if the 5650 CPAM license is not enabled. See the *5650 CPAM User Guide* for more information.

Table 2-1 describes the 5650 CPAM menus.

Table 2-1 5650 CPAM menus

Menu item	Description
Tools→Route Analysis	Access all 5650 CPAM management menus
Tools→Route Analysis→IGP topology	View the IGP topology map
Tools→Route Analysis→OSPF topology	View the OSPF topology map
Tools→Route Analysis→OSPFv3 topology	View the OSPFv3 topology map
Tools→Route Analysis→ISIS topology	View the ISIS topology map
Tools→Route Analysis→MPLS topology	View the MPLS topology map
Tools→Route Analysis→Flat Maps	View the following flat topology maps: • IGP Topology • OSPF Topology • OSPFv3 Topology • ISIS Topology • MPLS Topology • Multicast Topology
Tools→Route Analysis→IGP Network Data	View IGP network data

(1 of 2)

Menu item	Description
Tools→Route Analysis→BGP Network Data	View BGP network data
Tools→Route Analysis→Historical Routing Events	View the following historical routing events: • IGP • BGP
Tools→Route Analysis→Historical Routing Events→BGP Partition Manager	Access the BGP Partition Manager form
Tools→Route Analysis→Prefix List	View a list of advertised prefixes
Tools→Route Analysis→Path and Prefix Monitoring	Monitor paths and prefixes
Tools→Route Analysis→Managed Routes	View managed routes
Tools→Route Analysis→Checkpoints	View or create checkpoints
Tools→Route Analysis→Admin Domains / CPAAs	View admin domains and CPAAs
Tools→Route Analysis→Alarm Configuration	View or configure alarm settings
Tools→Route Analysis→CPAM Audit Manager	Access the CPAM Audit Manager form
Tools→Route Analysis→Simulated Impact Analysis	Create or manage scenarios
Tools→Route Analysis→Historical Impact Analysis	Configure historical impact analysis
Tools→Route Analysis→Multicast Manager	Access the Multicast Manager form
Tools→Synchronization Manager	Access the Synchronization Manager form
Help→5650 CPAM License Information	View the 5650 CPAM license information

(2 of 2)

2.3 Workflow for 5620 SAM and 5650 CPAM integration

1. Determine the 5650 CPAM device quantity and module requirements. Contact your Alcatel-Lucent representative for assistance.
2. Obtain the system ID of the station that is to host the integrated 5620 SAM and 5650 CPAM systems. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information.
3. Use the system ID to obtain a 5650 CPAM license from Alcatel-Lucent.
4. Perform one of the following:
   a. Add the 5650 CPAM to an existing 5620 SAM system. See Procedure 2-1 for more information.
   b. Specify the Inclusion of the 5650 CPAM during a 5620 SAM installation or upgrade. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information.
5. Restart each 5620 SAM GUI client to enable the 5650 CPAM GUI menus and functions. See chapter *5620 SAM User Guide* for more information.
6. Perform the required 5650 CPAM functions using GUI and OSS clients, as required. See the *5650 CPAM User Guide* and *5620 SAM XML OSS Interface Developer Guide* for more information.

2.4 5620 SAM and 5650 CPAM integration procedures

The following procedure describes how to configure 5620 SAM and 5650 CPAM integration.

Procedure 2-1 To add the 5650 CPAM to a 5620 SAM system

Perform this procedure to enable the 5650 CPAM functions in an existing 5620 SAM system. After you perform this procedure, the 5620 SAM and 5650 CPAM systems are integrated.

Caution — The 5650 CPAM license file required in this procedure must be based on the system ID used to generate the 5620 SAM license file. See the *5620 SAM User Guide* for information about viewing and exporting the license information. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about obtaining the system ID of a station.

Note 1 — In a redundant 5620 SAM system, you must perform this procedure on each main server station.

Note 2 — You can perform this procedure regardless of whether the 5620 SAM software on the main server is running.

Note 3 — After the integration, you must restart each GUI client to enable the 5650 CPAM menus and functions on the client.

1 Choose Help→5620 SAM License Information from the 5620 SAM main menu. The 5620 SAM License (Edit) form opens.

2 Record the Licensed System IDs values.

3 Close the 5620 SAM License (Edit) form.

4 Request a 5650 CPAM license file using the Licensed System IDs values recorded in step 2.

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

6 Open a console window.

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

8 Enter the following:

```
bash$ ./nmsserver.bash import_license license_file ↵
```

where *license_file* is the absolute file path of the 5650 CPAM license zip file from Alcatel-Lucent

The following prompt is displayed:

```
Detected a 5650 CPAM license key. Do you want to proceed?
(YES/no):
```

9 Enter the following:

YES ↵

The main server reads the license file, copies the license file to a backup location, and displays the following status information:

```
Importing 5650 CPAM license key...

Original license key file has been backed up to
/opt/5620sam/server/timestamp/CPAMLicense.zip

Done.
```

where *timestamp* is a directory name in the following format: yyyy.mm.dd-hh.mm.ss

The main server puts the updated license into effect and enables the 5650 CPAM. No further configuration is required.

10 Close the console window.

11 Verify the imported license information.

12 If a license parameter is incorrect, contact Alcatel-Lucent technical support for assistance.

2.5 5620 SAM and 5620 NM integration

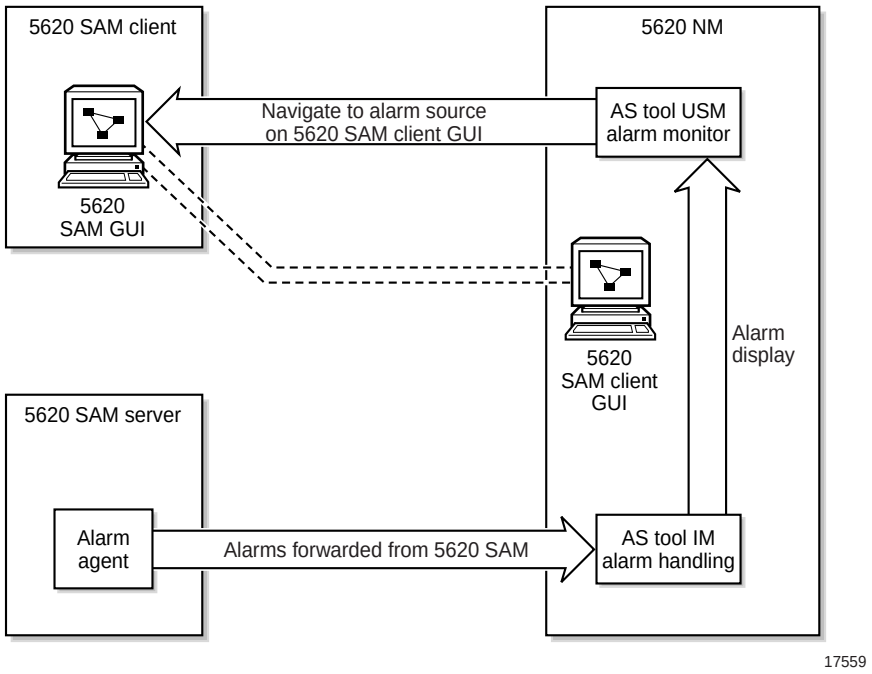
You can integrate the 5620 SAM and 5620 NM, which enables an operator to do the following.

- Navigate the 5620 SAM GUI using a 5620 NM client.
- Forward alarms from the 5620 SAM to the 5620 NM AS tool IM.
- Display 5620 SAM alarms graphically on the 5620 NM AS tool USM.
- Monitor services end-to-end using supported NM integration functions.

Note — Before you can integrate the 5620 SAM and 5620 NM, you must enable navigation from external systems during a 5620 SAM main server installation or upgrade, or enable it after an installation or upgrade using the 5620 SAM server configuration utility. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about enabling navigation from external systems.

Figure 2-1 shows how navigation to the 5620 NM and 5620 NM AS tool for alarm management occurs.

Figure 2-1 Alarm navigation



Before you start

Consider the following before you attempt to integrate the 5620 SAM and 5620 NM:

- The *5620 NM Release Notice* lists the 5620 SAM releases that are compatible with various 5620 NM releases.
- The 5620 NM and 5620 SAM integration software is in the 5620 SAM installation software file set.
- For 5620 SAM GUI navigation using a 5620 NM client, the 5620 SAM client must be installed on the same station that runs the 5620 NM client X-window access application.
- For alarm forwarding, the 5620 SAM and 5620 NM client software can be installed on the same or different stations.
- The platform for the 5620 NM software must meet the minimum requirements in the *5620 Network Manager Installation and Upgrade Guide*.
- You must configure the 5620 SAM to interwork with the 5620 NM software; for example, configure the 5620 SAM server to forward alarms and configure the 5620 SAM client to allow navigation from external systems.

5620 SAM client GUI startup and navigation restrictions

The following restrictions apply to 5620 SAM client GUI navigation using a 5620 NM client.

- When the client GUI is starting, 5620 NM navigation requests are blocked.
- A 5620 SAM client accepts navigation requests after the client GUI user logs in.

- Each navigation request is submitted only after a login timeout expires. This timeout helps to decrease the number of requests that are sent when a user submits and then immediately cancels a request.
- A 5620 SAM client delegate server acts as a single 5620 SAM client instance; you cannot configure a client delegate server to integrate with more than one 5620 NM client.
- The following navigation rules apply when multiple client GUIs are running.
  - A navigation request is cancelled when the client GUI is shut down.
  - All navigation requests are handled by the first registered client GUI.
  - If no client GUI is registered, a 5620 SAM server starts a new client GUI when it receives a navigation request.
  - If the currently registered 5620 SAM client GUI shuts down, another registered client GUI handles the navigation requests.

2.6 Workflow for 5620 SAM and 5620 NM integration

1. Ensure that the appropriate 5620 SAM integration software is installed and appropriately configured on the 5620 NM. See Procedure 2-2 for more information.
2. Configure the 5620 SAM client and server to support GUI navigation. See Procedure 2-3 for more information.
3. Start the 5620 SAM GUI. See the *5620 SAM User Guide* for more information.
4. Start the 5620 NM client GUI. See Procedure 2-4 for more information.
5. Perform the required network management function using the appropriate GUI, as described in section 2.5.

2.7 5620 SAM and 5620 NM integration procedures

The following procedures describe how to configure 5620 SAM and 5620 NM integration.

Procedure 2-2 To configure 5620 SAM and 5620 NM GUI integration

Perform this procedure to enable the use of a 5620 SAM client GUI through a 5620 NM client GUI.

1. Include the required 5620 SAM integration package in the 5620 NM installation. Consult the 5620 NM documentation for integration software installation and configuration information.
2. If required, configure the 5620 SAM server to forward alarms to the 5620 NM, as described in section 2.5.
3. If navigation from external systems is not currently enabled on each 5620 SAM main server, perform Procedure 2-3.

4 Install a 5620 SAM GUI client on a station that displays the 5620 NM client GUI. This is typically a station that runs an X-Window terminal emulator, but it can also be the 5620 NM database networkstation or the 5620 NM operator server networkstation, if a client GUI is locally displayed.

5 Perform one of the following on the station where the 5620 SAM client is installed.

a On a Solaris or RHEL station, open the *path*/nms-client.xml file with a plain-text editor

where *path* is the 5620 SAM client configuration directory, typically /opt/5620sam/client/nms/config

b On a Windows station, open the *path*/nms-client.xml file with a plain-text editor

where *path* is the 5620 SAM client configuration directory, typically C:\5620sam\client\nms\config

6 Perform the following steps to ensure that anti-aliasing is disabled.

i Search for the following XML tag that marks the beginning of the topologyMaps section:

```
<topologyMaps
```

ii Edit the antiAliasActive entry in the topologyMaps section to read “false” as shown below.

```
<topologyMaps
     iconReductionThreshold="40"
     labelHideThreshold="35"
        snapToGridInterval="25"
        antiAliasActive="false"
     />
```

7 Open a console window on the station.

8 Perform one of the following to run the navigator proxy script and start the client software.

a On a Solaris or RHEL station, perform the following steps.

i Enter the following at the CLI prompt:

```
# cd path
```

where *path* is the 5620 SAM client binary directory, typically /opt/5620sam/client/nms/bin

ii Enter the following:

./install_navigation_daemon.bash

iii Enter the following:

./nmsclient.bash

b On a Windows station, perform the following steps.

i Enter the following at the CLI prompt:

cd *path*

where *path* is the 5620 SAM client binary directory, typically C:\5620sam\client\nms\bin

ii Enter the following:

install_navigation_service.bat

iii Enter the following:

nmsclient.bat

The GUI client starts.

9 Use the 5620 SAM client GUI to create a 5620 NM user account that has a non-administrative privilege level with the appropriate scope of command role applied. See the *5620 SAM User Guide* for more information about configuring user accounts and how to apply a scope of command role.

10 Copy /opt/5620sam/server/nms/lib/common/generated/nms_common_core.jar from a 5620 SAM main server to the opt/netmgt/jnm/samjms/lib directory on the 5620 NM database networkstation.

11 Copy the following files from the /integration/5620NM/client/samadaptor directory in the 5620 SAM installation software file set to the /opt/netmgt/samadaptor/lib directory on the 5620 NM database networkstation:

- jbasiccomp.jar
- jnavapi.jar
- navrmi.jar
- samAdaptor.jar

12 Open the X-Window terminal emulator on the station that has the newly installed 5620 SAM client.

13 Log in to the 5620 NM operator server networkstation as a user with administrative privileges.

14 Open a console window on the 5620 NM operator server networkstation.

15 Start the 5620 NM client. The 5620 NM client GUI opens. The 5620 SAM client GUI is available as a 5620 NM main menu item.

16 Use the 5620 SAM client account created in step 9 to perform the required interworking functions, as described in described in section 2.5, and the *5620 Network Manager User Guide*.

Procedure 2-3 To enable navigation from external systems on a 5620 SAM main server

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

2 Open a console window.

3 Navigate to the directory that contains the 5620 SAM installation software.

4 Perform one of the following

a On a RHEL station:

i Enter the following:

```
# cd Linux ↵
```

ii Enter the following:

```
# ./ServerInstall_RHEL_R_r_revision.bin ↵
```

where
R_r is the release identifier, in the form *MAJOR_minor*
revision is the revision identifier, such as R1, R3, or another descriptor

b On a Solaris station:

i Enter the following:

```
# cd Solarisx86 ↵
```

ii Enter the following:

```
# ./ServerInstall_SolarisX86_SAM_R_r_revision.bin ↵
```

where
R_r is the release identifier, in the form *MAJOR_minor*
revision is the revision identifier, such as R1, R3, or another descriptor

The 5620 SAM server configuration utility opens, and displays the Introduction panel.

5 Click on the Next button.

6 Accept the terms of the license agreement in the “Software License Agreement” panel.

7 Click on the Next button.

8 Choose Main Server Configuration in the “Choose Installation Type” panel.

9 Click on the Next button.

10 Click on the Next button in each subsequent panel until the “Navigation from External Systems” panel is displayed.

11 Select the “Enable Navigation from External Systems” parameter.

12 Configure the “TCP port for accepting GUI navigation requests” parameter.

13 Click on the Next button.

14 Click on the Next button in each subsequent panel until the “Installation Complete” panel is displayed.

15 Click on the Done button to close the server configuration utility.

16 Enter the following to switch to the samadmin user:

```
# su - samadmin ↵
```

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

18 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The 5620 SAM main server reads the nms-server.xml file and puts the configuration changes into effect.

Procedure 2-4 To start the 5620 NM GUI

1 Log in to the 5620 SAM single-user client or client delegate station

2 Start the X-terminal software.

3 Use the X-terminal software to start the 5620 NM GUI on the station that has the 5620 NM Operator Position installed.

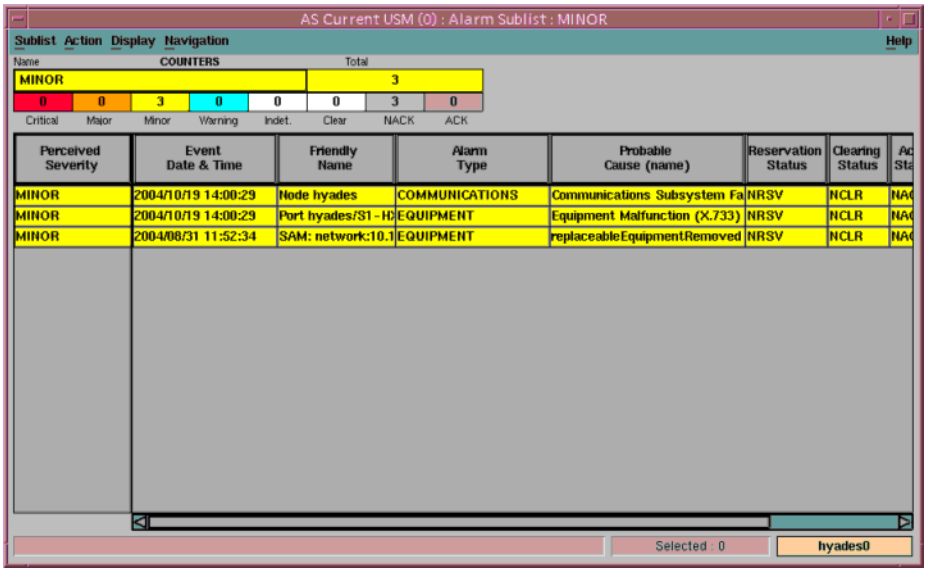
Procedure 2-5 To navigate from the 5620 NM AS tool USM to the 5620 SAM client GUI

See the *5620 SAM Troubleshooting Guide* for more information about troubleshooting using alarms.

1 Choose a counter summary window or alarm sublist from the AS tool USM.

2 Choose a sublist or an alarm in a sublist. 5620 SAM alarms are preceded by SAM in the Friendly Name field of the alarm sublist, as shown in Figure 2-2.

Figure 2-2 5620 SAM alarm in the AS tool USM



3 From the 5620 NM AS tool USM menu, choose Navigation→External Equipment→Show Equipment to navigate to the property form that lists the alarm on the 5620 SAM client GUI. The appropriate form is displayed. If the 5620 SAM client GUI is running, a new object properties form is displayed.

4 If the client GUI is not running, perform the following steps.

i Open the 5620 SAM client GUI.

ii View the object property form that is displayed on the 5620 NM client GUI.

5 After the alarm issue is resolved, clear the alarm using the 5620 SAM client GUI. Alarm status changes are shown in the 5620 NM AS tool USM.

2.8 5620 SAM and 9959 NPO integration

The 9959 NPO provides QoS information and cartographic tools for evaluating LTE RAN network performance and planning network expansion. When the 9959 NPO is discovered and by 5620 SAM, its QoS alerts be displayed as alarms in the 5620 SAM Alarm Window.

The 5620 SAM can manage the 9959 NPO as an EM system using the Horizontal Integration Protocol (HIP). When managed by the 5620 SAM, the 9959 NPO is displayed as an EM system in the equipment tree. Logical entities and 9959 NPO equipment are displayed as child objects of the parent EMS. See the *9959 Network Performance Optimizer (NPO) Administration User Guide* for information about 9959 NPO server configuration tasks that are required for integration with the 5620 SAM. See Procedure 2-6 for more information about discovering the 9959 NPO as a managed EM system. In the 5620 SAM GUI and documentation, the terms EMS and EM system are synonymous.

See the *5620 SAM LTE RAN User Guide* or the *5620 SAM LTE ePC User Guide* for information about viewing NPO alerts in the 5620 SAM GUI.

9959 NPO redundancy

The 5620 SAM supports 9959 NPO high availability through the management of redundant primary and secondary servers. In the event of a switchover, the new primary 9959 NPO server triggers a 5620 SAM resynchronization with both servers and the 5620 SAM updates the displayed alerts. The following behavior applies to 9959 NPO redundancy from a 5620 SAM perspective:

- The primary and secondary 9959 NPO servers must both be discovered as managed EMS. See Procedure 2-6.
- The secondary 9959 NPO server sends PMON alerts only. All QoS and real-time alert handling is done by the primary server.
- The 9959 NPO servers manage alert filtering between the primary and secondary to prevent alert duplication.
- The 9959 NPO servers manage all switchover triggering.
- The 5620 SAM periodically attempts to reconnect to an unreachable 9959 NPO server and triggers a resynchronization when the server is reachable.

See the *9959 Network Performance Optimizer (NPO) Administration User Guide* and related documentation for more information about managing 9959 NPO redundancy.

File transfer between the 5620 SAM and the 9959 NPO

The 9959 NPO retrieves files from 5620 SAM servers using the WebDAV protocol. You must enable WebDAV access during 5620 SAM server installation or reconfiguration, as this function is not enabled by default. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information. See Procedure 2-9 for information about viewing the status of the WebDAV protocol for a 5620 SAM main server.

East-West licensing for the 9959 NPO

NEs, hardware, and objects managed by a 9959 NPO EMS in the 5620 SAM network consume East-West license tokens. An East-West license token is consumed by each of the following object types when managed by the 9959 NPO:

- MME pools
- standby 5620 SAM servers
- PLMNs
- 9959 NPO servers

Note — Managing PLMNs with the 9959 NPO can consume a large number of East-West license tokens. Provisioned license capacity must be able to accomodate the expected number of managed PLMNs, which can be viewed using the 9959 NPO Analysis Desktop.

2.9 5620 SAM and 9959 NPO integration procedures

Perform the procedures in this section to manage 9959 NPO integration with the 5620 SAM.

Procedure 2-6 To discover the 9959 NPO as an EM system

Note — You must specify a topology group other than the default Discovered NEs group when discovering an EM system. Step 1 of this procedure describes a basic process for creating a topology group. See the *5620 SAM User Guide* for more information about creating and populating topology groups.

1 If required, create a topology group for the EM system:

- **i** Choose Create→Equipment→Group from the 5620 SAM main menu. The Group (New Instance) (Create) form opens.
- **ii** Configure the parameters:
  - Name
  - Description
  - Background Image
- **iii** Click on the OK button. The form closes and the topology group is displayed in the navigation tree and topology map.

2 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens with the Discovery Rules tab displayed.

3 Click on the Create button. The Create Discovery Rule form opens with the Specify General Attributes step displayed.

4 Click on the Select button for the Group Name, select a topology group other than Discovered NEs, and click on the OK button. The form is updated with the group name.

5 Click on the Next button until the Add EM Systems step is displayed.

6 Perform the following steps to complete the Add EM Systems step:

- **i** Click on the Create button. The EM System (Create) form opens with the General tab displayed.
- **ii** Configure the parameters:
  - Auto-Assign ID
  - ID
  - Element Manager System Name
  - Description
- **iii** Click on the Element Managers tab.
- **iv** Click on the Create button. The Element Manager (Create) form opens.

v Configure the parameters:

- Host Name
- Server IP Address
- Server Port Number
- User Name
- Password
- Confirm Password

Note — You cannot enter a hostname as the value of the Server IP Address parameter.

vi Click on the OK button. The Element Manager (Create) form closes and a dialog box opens.

vii Click on the OK button.

viii Click on the OK button. The EM System (Create) form closes and a dialog box opens.

ix Click on the OK button.

7 Click on the Finish button. The Create Discovery Rule form closes and a dialog box opens.

8 Click on the OK button.

9 Click on the Apply button in the Discovery Manager (Edit) form. A dialog box opens.

10 Click on the Yes button. The discovery rule is saved.

11 Activate the EMS discovery:

Note — The 5620 SAM does not discover an EM system until you set the Administrative State parameter of the EMS object to Up and save the changes in the Discovery Manager.

i In the Discovery Manager (Edit) form, click on the EM Systems tab.

ii Choose the EM system you created in step 6 and click on the Properties button. The EM System (Edit) form opens with the General tab displayed.

iii Set the Administrative State parameter to Up.

iv Click on the OK button. The EM System (Edit) form closes.

v Click on the Apply button in the Discovery Manager (Edit) form. A dialog box appears.

vi Click on the Yes button. The changes are saved and the 5620 SAM attempts to discover the EM system.

12 Close the Discovery Manager (Edit) form.

Procedure 2-7 To unmanage and delete the 9959 NPO from the 5620 SAM network

Warning 1 — Deleting an EMS results in a loss of management data and completely removes the EMS from the managed network. See the *5620 SAM User Guide* for more information.

Warning 2 — Deleting the 9959 NPO from the network clears all alarms raised by the 9959 NPO and all alarms raised by the 5620 SAM against the 9959 NPO.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens with the Discovery Rules tab displayed.

2 Click on the EM Systems tab.

3 Configure the filter criteria, if required, and click on the Search button.

4 Choose an EMS and click on the Properties button. The EM System (Edit) form opens with the General tab displayed.

5 Set the Administrative State parameter to Down.

6 Click on the OK button. The EM System (Edit) form closes.

7 Choose the administratively down EM system and click on the Delete button. A dialog box opens.

8 Click on the Yes button. The EM system is deleted.

9 Close the Discovery Manager (Edit) form.

2.10 5620 SAM and EM systems integration

The 5620 SAM can manage multiple element manager systems using the Horizontal Integration Protocol (HIP). The HIP allows EM systems to integrate with the 5620 SAM using a single jar file (the HIP library jar file). When integrated with the 5620 SAM, the EM system's inventory and alarm information are displayed in the 5620 SAM GUI. Any operations performed on the EM system's alarms using the 5620 SAM GUI are then sent to the EM system for processing, where they can be accepted or denied. The HIP also enables EM system alarms to be pushed directly onto 5620 SAM NEs. For more information about discovering EM systems, see the *5620 SAM User Guide*.

The HIP library jar file is provided with the 5620 SAM and must be installed in the project classpath. Two versions are delivered: one compiled with Java 1.6 and one compiled with Java 1.7. Only one of these may be used at a time. The HIP library jar file contains all required classes, a default logger, and two simulators. The EM system simulator can be used as an example for EM system development. The 5620 SAM simulator simulates a 5620 SAM connecting to an EM system and performing an initial resynchronization.

The user must create the HipServerImpl class, which will be dedicated to communication between the HIP server (located on the EM system server) and the HIP client (located on the 5620 SAM server), and the HipClientInterface callback. The HipServerImpl class will contain all the necessary facilities to connect via Cproto and to call HIP methods, as well as the HipClientInterface callback. All requests coming from the HIP client will arrive on the HipClientInterface callback.

Cproto is the protocol that is used to establish a session between the HIP server and the HIP client. It uses two seperate channels for events and requests. Cproto is based on TCP protocol and Java API NIO.

2.11 5620 SAM and 5670 RAM integration

The 5670 RAM server processes AA statistics. The 5620 SAM statistics collector - which can be an auxiliary 5620 SAM server - prepares the statistics files which are retrieved by the 5670 RAM. The 5620 SAM statistics collection intervalizes the statistics before they are retrieved by the 5670 RAM.

See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information about how to enable application assurance statistics collection on the 5620 SAM and how to install the 5670 RAM statistics adaptor component on the 5620 SAM.

See the *5620 SAM User Guide* for more information about application assurance and application assurance policies.

Procedure 2-8 To enable 5670 RAM support

Perform this procedure to enable the 5670 RAM functions on a 5620 SAM system. You require samadmin user privileges to perform this procedure.

1. Peform one of the following:
   a. If the 5620 SAM server is deployed in a standalone configuration, perform step 2 on the main server.
   b. If the 5620 SAM server is deployed in a redundant configuration, perform step 2 on the primary main server.
2. Log in to the main server station as the samadmin user.
3. Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.
4. Create a backup copy of the nms-server.xml file.
5. Open the nms-server.fml file using a plain-text editor.

Caution — Contact your Alcatel-Lucent techincal support representative before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

6. Locate the following section:

```
<ram5670

ramEnabled="false" />
```

7 Change “false” to “true”.

8 Save and close the nms-server.xml file.

9 Open a console window.

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

11 Perform one of the following:

a If you are configuring a main server in a standalone deployment or the primary main server in a redundant deployment, enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

b If you are configuring the standby main server in a redundant deployment, enter the following at the prompt:

```
bash$ ./nmsserver.bash force_restart ↵
```

The main server restarts and puts the configuration change into effect.

12 Log out of the main server.

13 If the 5620 SAM server is deployed in a redundant configuration, perform steps 2 to 12 on the standby main server.

14 Close the open console windows.

2.12 5620 SAM and 9952 WPS integration

File transfer between the 5620 SAM and the 9952 WPS

The 9952 WPS transfers files to and from 5620 SAM servers using the WebDAV protocol. You must enable WebDAV access during 5620 SAM server installation or reconfiguration, as this function is not enabled by default. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information. See Procedure 2-9 for information about viewing the status of the WebDAV protocol for a 5620 SAM main server.

You can set up the automatic transfer of CM XML files between the 5620 SAM and the 9952 WPS by enabling the server repository function of the 9952 WPS. Manual transfer via FTP is also supported. See the *9952 WPS User Guide* for more information about the server repository function.

Note — Alcatel-Lucent recommends enabling SSL on the 5620 SAM main server before using the server repository function of the 9952 WPS to import and export CM XML files. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about configuring SSL.

Procedure 2-9 To view WebDAV activation status on a 5620 SAM main server

Perform this procedure to verify whether the WebDAV protocol for file transfers to the 9952 WPS and 9959 NPO is enabled.

1. Log in to a main server station as the samadmin user.
2. Open a console window.
3. Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.
4. Enter the following command:

   ```
   bash$ ./nmsserver.bash -s nms_status ↵
   ```

5. Verify that the following status message is displayed:

   ```
   -- WebDAV Access to Activation Data Enabled
   ```

6. If the message is not displayed, enable WebDAV during a 5620 SAM server reconfiguration. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about enabling the WedDAV protocol.
7. Close the console window.

2.13 5620 SAM and 5780 DSC integration

The 5780 DSC is treated as a device that is managed by the 5620 SAM, rather than an external system that requires integration with the 5620 SAM. The 5620 SAM allows you to view the properties for the equipment, instance, Diameter proxy agent, and policy charging rules for the 5780 DSC. The 5780 DSC is represented in the 5620 SAM equipment navigation tree. The instance, Diameter proxy agent, and policy charging rule properties are viewable using the Manage→Mobile Core→DSC Instances 5620 SAM main menu option.

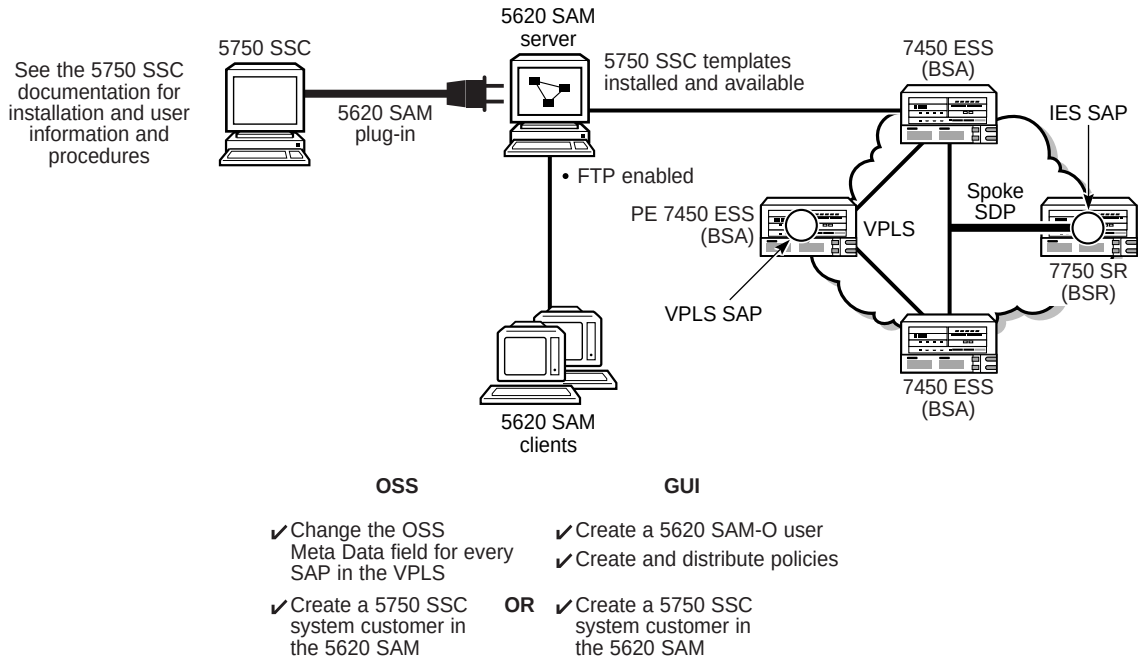
The *5620 SAM LTE ePC User Guide* describes 5780 DSC discovery and management using the 5620 SAM.

2.14 5620 SAM and 5750 SSC integration

The 5620 SAM can be configured to interoperate with the 5750 Subscriber Services Controller. The 5750 SSC provides centralized control of subscriber access services for triple play service delivery; for example, DHCP to identify subscribers and trigger service configuration.

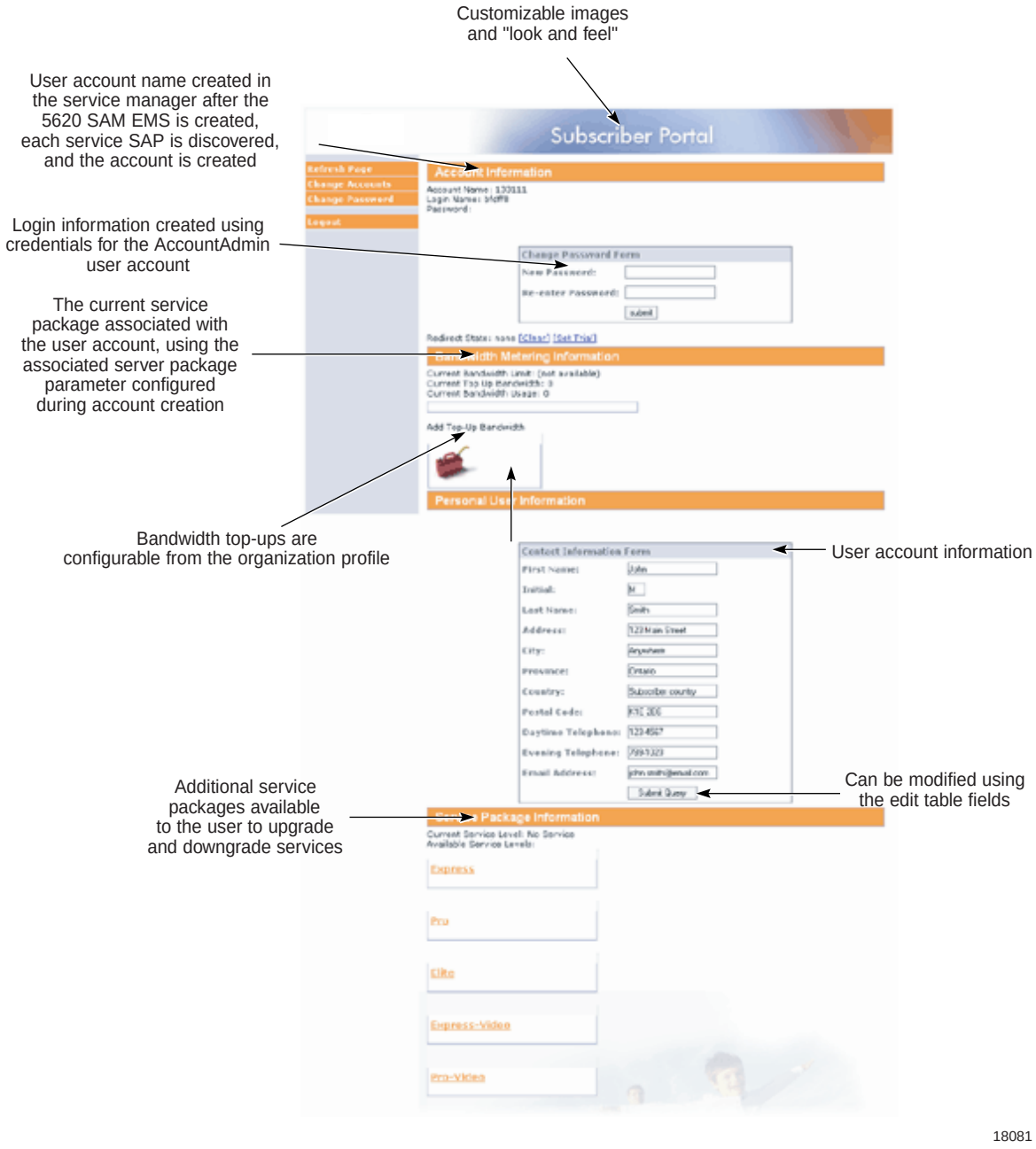
Figure 2-3 shows the integration requirements for the 5620 SAM and the 5750 SSC. See the 5750 SSC documentation suite for information about how to configure application interoperation.

Figure 2-3 5750 SSC and 5620 SAM integration



You use the 5750 SSC Service Manager to create and manage subscriber services, including user account information and QoS levels. The 5750 SSC user accounts represent the residential subscribers of triple play services. The information configured in the 5750 SSC Service Manager is used to build the subscriber web portal for user self-management. Figure 2-4 shows a subscriber web portal and how the component pieces are assembled from 5750 SSC subscriber management configurations.

Figure 2-4 Subscriber web portal



2.15 5620 SAM and 5520 AMS integration

A 5620 SAM client GUI can discover and monitor other element manager systems, including the 5520 AMS. When discovered as a managed EMS, the 5520 AMS can forward alarms raised against a 7705 SAR-M. These alarms are then correlated and shown against the corresponding network element within the 5620 SAM client GUI.

2.16 Call trace data transfer to the 9958 WTA

The 5620 SAM supports automatic and secure call trace data file transfer to the 9958 WTA over HTTPS via the WebDAV protocol. The transfer function uses the login credentials of a 5620 SAM user, and facilitates call trace file management by removing the need for manual transfers over SFTP. The following conditions must be true to use the call trace data file transfer function:

- SSL is enabled on all call trace auxiliary servers. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about configuring SSL.
- A 5620 SAM user with read access to the calltrace.WebDAVSharedData permission is available. See the *5620 SAM System Administrator Guide* for more information about creating 5620 SAM users, configuring scope of command roles, and for lists of assignable permissions.

Note — Read access is the only required access type for the calltrace.WebDAVSharedData permission.

- Configuration for data collection from the 5620 SAM to the 9958 WTA using the login credentials of a 5620 SAM user is complete. See the *9958 Wireless Trace Analyzer Installation and User Guide for LTE and W-CDMA* for more information about configuring data collection.

3 — 5620 SAM integration with Single Sign On

3.1 SSO integration

Single Sign On (SSO) technology enables a user to access all resources within a domain after having entered their credentials just one time. SSO uses centralized authentication servers to ensure that users do not need to enter their credentials repeatedly. Security is provided on all levels without the inconvenience of re-prompting users.

Note — Users who access the 5620 SAM client GUI through Internet Explorer must deselect the "Do not save encrypted pages to disk" Security option. This option is on the Advanced tab of the Internet Options form, which is accessible from the Tools menu.

You can use SSO to integrate the 5620 SAM and the following systems:

- SANE portal
- 1350 OMS
- OMC-RAN

3.2 SSO integration procedures

Use the following procedures to enable 5620 SAM SSO integration with other systems.

Procedure 3-1 To configure 5620 SAM and LSM portal integration

Perform this procedure to configure a 5620 SAM system for interworking with the LSM portal. The LSM portal is a component used for integration with the 1350 OMS. Ensure that the 5620 SAM Server is stopped before you begin. You require the following user privileges on each main server station to perform this procedure:

- root
- samadmin

The following steps assume that the 5620 SAM server is installed at /opt/5620sam/server. Modify paths accordingly if your 5620 SAM server is installed to a different location.

1 Deploy the csa_v2_proxy_spi.sar file.

```
/opt/5620sam/server/nms/jboss/server/default/deploy/csa_v2_proxy
_spi.sar

# cp -i
/opt/5620sam/server/nms/jboss/sso/csa/csa_v2_proxy_spi.sar
/opt/5620sam/server/nms/jboss/server/default/deploy/csa_v2_proxy
_spi.sar

# chown samadmin:sam
/opt/5620sam/server/nms/jboss/server/default/deploy/csa_v2_proxy
_spi.sar
```

2 Modify the following fields within /5620sam/sever/nms/config/sso/csa_proxy_config_service.xml:

   i Set the ipaddress parameter to the IP address of the LSM Portal. Contact your LSM Portal administrator to obtain.

   ii Set the port parameter to the port number of the LSM Portal. Contact your LSM Portal administrator to obtain.

3 Go to /opt/5620sam/server/nms/config/clientDeploy/nms-client.xml and add the following lines in the <integration> section:

```
lsmproperties="https://<pathToLsmApiProperties>"
applicationid="<applicationIdValue>"
```

Note 1 — <pathToLsmApiProperties> is the URL of the path to the LSM Portal LSM API properties file. Contact your LSM Portal administrator to obtain.

Note 2 — <applicationIdValue> is the value of the 5620 SAM target binding ID configured in the LSM Portal. Contact your LSM Portal administrator to obtain

4 When communication to the LSM Portal is SSL secured, perform the following steps to share the LSM Portal security certificates with the 5620 SAM server and its clients:

   i Obtain the public security certificate from the LSM Portal administrator.

   ii Import this certificate into the 5620 SAM server truststore found at /opt/5620sam/server/nms/config/ssl/trustStore/cacerts.trustStore.

   iii Go to /opt/5620sam/server/nms/bin/setenv.rc and set the SSL path parameter to the path of the 5620 SAM server truststore.

   iv Go to /opt/5620sam/server/nms/config/clientDeploy/setenv.bat and uncomment the following line:

```
rem  set
JVM_OPTIONS_SSL=-Djavax.net.ssl.trustStore=..\config\ssl\tru
stStore\cacerts.trustStore
```

   v Go to /opt/5620sam/server/nms/config/clientDeploy/setenv.rc and uncomment the following line:

```
#JVM_OPTIONS_SSL="-Djavax.net.ssl.trustStore=../config/ssl/t
rustStore/cacerts.trustStore"
```

   vi To deploy the changes, run the following command as the samadmin user:

```
bash$ /opt/5620sam/server/nms/bin/nmsdeploytool.bash deploy
```

5 Restart the 5620 SAM server.

Procedure 3-2 To configure 5620 SAM integration with a system that uses the LSM portal

Perform this procedure to configure a 5620 SAM system to allow navigation requests from an external system that uses the LSM portal.

Note — You must perform this procedure on each main server in the 5620 SAM system.

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

2 Open *path*/nms/config/sso/em_lsmproxy_config.xml using a plain-text editor.

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

3 Locate the following XML tag, which marks the beginning of the section that lists each external system, or target application, that connects to the 5620 SAM through the LSM portal, as shown in Code 3-1.

Code 3-1: Beginning of target applications section

```
<lsm-proxy-target-applications>
```

The section contains multiple target application entries in separate subsections. By default, each entry is populated with sample values, and the group of entries is surrounded by comment tags to disable them.

4 To configure a target application, edit the subsection directly below the leading comment tag, which is the first line in Code 3-2, to read as shown in Code 3-2.

Code 3-2: Target application subsection

```
<!--
    <target-application>
        <em-server>
            <servertype>serverType</servertype>
            <server-ip>serverIP</server-ip>
        </em-server>
        <jnlp-url>JNLP_URL</jnlp-url>
    </target-application>
```

where

serverType: is the application type, for example, OMC-RAN

serverIP is the public IPv4 address of the server application on the external system

JNLP_URL is the URL of the JNLP file required to run the client application; see the external system documentation for the file location

5 To enable the target application, move the leading comment tag line to the line directly below the closing tag of the target application subsection, as shown in Code 3-3.

Code 3-3: Enabled target application

```
    </target-application>
```

<! - -

6 Save and close the file.

Procedure 3-3 To configure 5620 SAM and SANE portal integration

Perform this procedure to configure a 5620 SAM system for interworking with the SANE portal. You require the following user privileges on each main server station to perform this procedure:

- root
- samadmin

Caution — If you are using this procedure to reconfigure one or more installed main servers, the following conditions apply:

- If the main servers do not currently have SSL enabled, you must prepare the 5620 SAM system for operation with SSL. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about configuring SSL.
- The procedure requires that you stop and restart each main server, which causes a network management outage. Ensure that you perform this procedure only during a scheduled maintenance period.

In a redundant deployment, the sequence of events is the following:

- standby main server stopped
- standby main server reconfigured
- standby main server started
- primary main server stopped / server activity switch triggered
  This is the beginning of the network management outage.
- server activity switch completes
  This is the end of the network management outage.
- primary main server reconfigured
- primary main server started
- if required, manual activity switch performed to restore initial primary and standby main server roles

Note 1 — You can perform this procedure as part of a 5620 SAM main server installation or upgrade, or as a configuration activity on an installed main server.

Note 2 — You must perform this procedure on each main server In a redundant 5620 SAM deployment, in the following order:

- standby main server
- primary main server

1 Perform one of the following.

a If you are performing this procedure as part of a main server installation or upgrade, perform the initial installation or upgrade procedure steps in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* up to, but not including, the step that describes opening the 5620 SAM server installer.

b If you are performing this procedure to reconfigure one or more installed main servers, perform the following steps.

i Log in to the main server station as the samadmin user.

ii Open a console window.

iii Enter the following to change to the server binary directory:

```
bash$ cd path/nms/bin ↵
```

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

iv Enter the following to stop the 5620 SAM main server software:

```
bash$ ./nmsserver.bash stop ↵
```

v Enter the following to display the 5620 SAM main server status:

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

The command displays a status message.

vi The 5620 SAM main server is stopped when the command displays the following status message:

```
Application Server is stopped
```

If the command displays a different message, wait 5m and repeat step 1 b v. Do not proceed to the next step until the server is stopped.

vii Enter the following to switch to the root user:

```
bash$ su - ↵
```

viii Navigate to the directory that contains the 5620 SAM installation software.

2 Perform one of the following to open the 5620 SAM server configuration utility.

a On a RHEL station:

i Enter the following:

cd Linux ↵

ii Enter the following:

./ServerInstall_RHEL_*R_r_revision*.bin -DconfigSANE=yes ↵

where
R_r is the release identifier, in the form *MAJOR_minor*
revision is the revision identifier, such as R1, R3, or another descriptor

b On a Solaris station:

i Enter the following:

cd Solarisx86 ↵

ii Enter the following:

./ServerInstall_SolarisX86_SAM_*R_r_revision*.bin -DconfigSANE=yes ↵

where
R_r is the release identifier, in the form *MAJOR_minor*
revision is the revision identifier, such as R1, R3, or another descriptor

3 Accept the terms of the license agreement in the "Software License Agreement" panel.

4 Click on the Next button. The "Choose Installation Type" panel is displayed.

5 Perform one of the following.

a If you are performing this procedure as part of a main server installation or upgrade, select "Main Server Installation" in the "Choose Installation Type" panel.

b If you are performing this procedure to reconfigure an installed main server, select "Main Server Configuration" in the "Choose Installation Type" panel.

6 Click on the Next button.

7 Perform one of the following.

a If you are performing this procedure as part of a main server installation or upgrade, perform the subsequent installation or upgrade procedure steps described in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* until the "SSL Configuration" panel is displayed.

b If you are performing this procedure to reconfigure an installed main server, click on the Next button in each subsequent panel until the "SSL Configuration" panel is displayed.

8 Select the "Enable Secure Communication" parameter.

Note — You must enable and configure SSL before you can enable or configure SANE SSO.

9 Configure the remaining parameters on the panel.

10 Click on the Next button. The "SANE SSO Configuration" panel is displayed.

11 Select the "Enable SANE SSO" parameter.

12 Configure the "Windows Client Installation Directory" parameter by specifying the 5620 SAM software installation directory used for Windows clients.

13 Configure the "Unix Client Installation Directory" parameter by specifying the 5620 SAM software installation directory used for Solaris clients.

14 Configure the "Enable Response Signature Validation" parameter.

15 Click on the Next button. The "SANE SSO Certificate Files Configuration" panel is displayed.

16 Click on the Add button to specify an SSO certificate file. A file browser opens.

17 Choose a certificate file and click on the OK button.

18 Repeat steps 16 and 17 to specify an additional certificate file, if required.

19 Click on the Next button.

20 Perform one of the following.

a If you are performing this procedure as part of a main server installation or upgrade, perform the subsequent installation or upgrade procedure steps described in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

b If you are performing this procedure to reconfigure an installed main server, perform the following steps.

i Click on the Next button in each subsequent panel until the "Installation Complete" panel is displayed.

ii Click on the Done button to close the server installer.

iii Enter the following to switch back to the samadmin user:

```
# exit ↵
```

iv Enter the following to start the 5620 SAM main server:

```
bash$ ./nmsserver.bash start ↵
```

The 5620 SAM main server restarts and puts the SANE SSO configuration into effect.

- If required, perform a manual server activity switch to restore the initial primary and standby main server roles.

Procedure 3-4 To enable SSO between 5620 SAM and an identity provider using v1.1 SAML artifacts

You require the following user privileges on each main server station to perform this procedure:

- root
- samadmin

1. Log in to the main server station as the samadmin user.
2. Open a console window.
3. Enter the following to add the metadata file:

```
# cd /opt/5620sam/server/nms/config/sso/metadata/1.1/ ↵

# cp -p idp_metadata.xml  idp_metadata.orig ↵

# vi idp_metadata.xml ↵
```

4. Configure the parameters as follows:

```
entityId = http://identity_provider_IP:8080/openam_954

singleSignOnServiceLocation.POST =
http://identity_provider_IP:8080/openam_954/SAMLPOSTProfileServl
et

singleSignOnServiceLocation.ARTIFACT =
http://identity_provider_IP:8080/openam_954/SAMLAwareServlet

artifactResolutionServiceLocation =
http://identity_provider_IP:8080/openam_954/SAMLSOAPReceiver

certificateFileLocation =

sourceID=EAJOXo5wCRwB9/30i3hUkkJIthE=
```

where
identity_provider_IP is the IP address of an identity provider using v1.1 SAML artifacts

Note — The values of the entityId and sourceID parameters will vary depending on the specific configuration of your identity provider.

5 Enter the following to configure the SAML.properties file:

 # vi /opt/5620sam/server/nms/jboss/server/default/deployAlcatel5620SRM/z_z_z/webSSO.war/WEB-INF/classes/config/SAML.properties ↵

6 Configure the parameters as follows:

```
com.alu.cnm.csa.saml.sp.signValidatorMarshaller = OPENSAML
```

4 — 5620 SAM integration with CFMA

4.1 CFMA integration overview

The SAM-CFMA adapter translates 5620 SAM alarms into alarms for CFMA. The adapter connects to the 5620 SAM using a 5620 SAM-O JMS connection. The connection parameters are specified in an XML configuration file. The password in the XML file is MD5-hashed. The adapter software is in the integration/samcfmadapter directory of the 5620 SAM software installation file set.

An installed SAM-CFMA adapter must be of the same release as the 5620 SAM server with which it is to interface, and the 5620 SAM and CFMA releases must be compatible. The 5620 SAM and CFMA clocks must be synchronized to ensure that the JMS connection functions correctly and the alarm timestamps match on each system. Alcatel-Lucent recommends that both systems synchronize their time using the same NTP server.

The sam-cfma-adapter.sar file is an archive of the required files for SAM-CFMA adapter support. A CFMA system administrator must extract the file contents and deploy them to the correct CFMA directory. Contact Alcatel-Lucent technical support for more information.

4.2 CFMA integration procedures

Use the following procedures to install the 5620 SAM adapter for CFMA.

Procedure 4-1 Installing the SAM-CFMA adapter sar file

The paths to the configurations provided in the following procedure are provided as an example only and may vary, depending on the CFMA installation and version. Consult the CFMA documentation for details.

1 Run the following command:

```
cd <JBOSS_dir>/alu_cnm_cfma_main/deploy
```

2 To create the SAM-CFMA adapter directory, run the following command:

```
mkdir sam-cfma-adapter.sar
```

3 To copy the sar file in the created directory, run the following commands:

```
cp <SAR_FILE_LOCATION>/sam-cfma-adapter.sar
<JBOSS_dir>/alu_cnm_cfma_main/deploy/sam-cfma-adapter.sar/

cd <JBOSS_dir>/alu_cnm_cfma_main/deploy/sam-cfma-adapter.sar/
```

4 To unzip the sar file, run the following command:

```
unzip sam-cfma-adapter.sar
```

5 To remove the unzipped sar file, run the following command:

```
rm sam-cfma-adapter.sar
```

Procedure 4-2 Setting CFMA preferences

The paths to the configurations provided in the following procedure are provided as an example only and may vary, depending on the CFMA installation and version. Consult the CFMA documentation for more information.

1 To set the EVENT_PROCESSING_WITH_DEVICETIME to true for the main and player servers, run the following commands:

```
cnm-preference-modify -c cfma -i main -d ../main/data/output
"/cfma/server/asset/main/com/alu/cnm/cfma/ngfm/server/fmcommon:E
VENT_PROCESSING_WITH_DEVICETIME:true"

cnm-preference-modify -c cfma -i main -d ../main/data/output
"/cfma/server/asset/player/com/alu/cnm/cfma/ngfm/server/fmcommon
:EVENT_PROCESSING_WITH_DEVICETIME:true"
```

2 To set the synchTimeout to 60, run the following command:

```
cnm-preference-modify -c cfma -i main -d ../main/data/output
"/cfma/server/asset/main/com/alu/cnm/cfma/ngfm/server/fmcollecto
r:synchTimeout:60"
```

Note — An initial discovery that takes more than 60 minutes requires increasing the synchTimeout.

Procedure 4-3 Enabling 5620 SAM server communication

Included in the sam-cfma-adapter.sar file is the jboss-service.xml configuration file. Prior to deploying the SAM-CFMA adapter, the following parameters within the jboss-service.xml configuration file must be modified to allow communication with the 5620 SAM server.

1 Open the jboss-service.xml configuration file.

2 Set the ipAddressOne parameter to the IP address of the primary 5620 SAM server.

3 Set the httpPortOne parameter to the HTTP port of the primary 5620 SAM server used for OSS requests.

4 Set the jndiPortOne parameter to the JNDI port of the primary 5620 SAM server.

5 Set the ipAddressTwo parameter to the IP address of the redundant 5620 SAM server.

6 Set the httpPortTwo parameter to the HTTP port of the redundant 5620 SAM server used for OSS requests.

7 Set the jndiPortTwo parameter to the JNDI port of the redundant 5620 SAM server.

8 Set the adapterType parameter to either 5620OMS or 5620XMS.

Note — This value is dependent on specific system integration.

9 Set the username parameter to the 5620 SAM user used for the OSS/JMS connections.

Note 1 — This user must be configured in the 5620 SAM server and must have OSS privileges.

Note 2 — In 5620 SAM, this user should be bound to a Span Profile that contains spans defining all alarmable objects for which the CFMA user wishes to receive alarm events.

Note 3 — Do not specify a Span Profile containing blocked spans as this will cause the SAM-CFMA adapter to become out of sync with the 5620 SAM.

10 Set the password parameter to the MD5 hashed password required for the 5620 SAM username.

11 Set the spanIds to a comma separated list of numeric values corresponding to span numbers configured on the 5620 SAM Server.

Note 1 — The span numbers specified here must match those belonging to the Span Profile of the 5620 SAM user specified in step 9.

Note 2 — Only alarms raised on objects belonging to the specified spanIds will be shown in CFMA.

Note 3 — Spans used by the SAM-CFMA adapter should not be modified after an interface is established between 5620 SAM and CFMA. Alarmed objects should not be added, removed, or moved from one span to another (i.e. move an NE from one group belonging to a spanId to another group belonging to a different spanId). Doing so will cause the CFMA alarm list to become out of sync with the 5620 SAM alarm list. If the CFMA alarms become out of sync with the 5620 SAM alarms, the 5620 SAM alarms can be synchronized from the CFMA GUI by performing Actions→Synchronize→Alarms and selecting the 5620SAM entry.

12 Restart the CFMA.

5 — 5620 SAM integration with Chronos SyncWatch

5.1 5620 SAM synchronization

The 5620 SAM supports IEEE 1588 PTP clocks for packet-based timing synchronization from a primary clock to one or more secondary clocks in a network. You can use the 5620 SAM to configure primary or secondary PTP clocks on network elements that support timing references. See the *5620 SAM User Guide* for more information about configuring IEEE 1588 PTP clocks.

You can use the 5650 CPAM to manage synchronization domains and assign IP path monitors to PTP peers. See the "Synchronization management" chapter in the *5650 CPAM User Guide* for more information.

The SyncWatch Probe provides a system for synchronization testing and monitoring for telecoms. The NetSMART Server component provides remote management of multiple SyncWatch Probes. The component collects data that can be used to alert users to potential synchronization problems. The 5620 SAM provides integration support for both the SyncWatch Probe and the NetSMART Server components. The 5620 SAM provides basic network element management support at the GNE level for the probe, as well as a fault management framework to manage synchronization-related alarms.

5.2 Synchronization overview

Networks monitor timing synchronization to ensure communications equipment operates in unison. Digital data is transmitted in discrete bits, data frames, or packets. When the data is transmitted through a communications network, synchronization ensures that each node and link is operating in phase. Synchronization helps ensure that data is not dropped or retransmitted.

Synchronization is critical for maintaining the correct operation and air frequency of telecom networks and services including SDH/SONET, ATM, 2G/3G mobile backhaul and PSTN voice services. IEEE 1588v2 synchronization is a low-cost layer 2/3 synchronization solution. SyncE is a low-cost physical layer synchronization solution.

Clocks

Network clocks at the sending and receiving sites control the rate at which data is transmitted and received. Timing synchronization ensures that the clocks on the source and target nodes are operating in unison. When the clocks are synchronized, the receiver more effectively reads the transmitted data. Synchronized clocks result in less dropped or retransmitted traffic.

Clocks can become out-of-synchronization when timing accuracy is not precise. Phase movements such as jitter and wander can effect network clocks, which are distributed among network elements. When timing synchronization deteriorates, service quality is impacted.

Network synchronization

Networks often use a hierarchical redundancy setup to synchronize their network elements. The primary reference clock is used as the timing reference for all secondary clocks in the network. A network element with the most reliable clock is usually designated as the primary reference clock. Secondary clocks adjust to the timing reference received from the primary clock and retransmit that timing reference to other secondary clocks.

Secondary clocks usually have more than one timing reference clock higher in the sync hierarchy. If the primary reference clock stops transmitting, the secondary clock switches over to a standby timing reference.

Primary reference clocks

Primary reference clocks must meet international standards for long-term frequency accuracy better than 1 part in 10. Atomic clocks are often used as primary reference clocks. A primary reference clock in a packet network is called a grandmaster clock. Grandmaster clocks transmit synchronization information in IEEE 1588v2 PTP timing packets.

Secondary clocks

A secondary clock maintains timing by receiving synchronization information from a reference clock. The secondary clock reproduces the timing received from the primary reference clock and maintains the timing reference even when the primary reference clock stops sending synchronization packets for a period.

Monitoring synchronization

Network elements often have capabilities for monitoring synchronization. You can also use monitoring applications specifically designed to troubleshoot network synchronization. Some independent synchronization monitoring applications and devices have their own timing reference with which to provide a measure of performance and reliability for the timing references in the network.

5.3 5620 SAM and Chronos SyncWatch integration overview

The 5620 SAM provides limited SNMP management support for GNEs. This support includes the following:

- discovery and display on topology maps
- inclusion in the navigation tree
- physical link creation and representation
- generic trap translation into 5620 SAM alarms
- status polling

The 5620 SAM extends GNE support for the Chronos SyncWatch and the NetSMART Server with an automated script bundle. The script bundle executes several scripts to automatically create GNE profiles and associated objects for the NetSMART Server and the SyncWatch Probe.

5.4 Alarm support

By default, the 5620 SAM supports a limited number of standard system and interface SNMP traps for GNEs. The 5620 SAM monitors SNMP reachability and interface status, and raises a standard alarm for each the following events:

- coldStart—the GNE restarts
- linkDown—an interface goes out of service
- linkUp—an interface returns to service

The 5620 SAM also supports GNE alarm catalogs to import SyncWatch Probe traps from the NetSMART Server and translate them into 5620 SAM alarms. An alarm catalog is a set of trap-to-alarm mappings that can be associated with a GNE profile. A GNE profile can have at most one alarm catalog, but each catalog can contain up to 150 alarm mappings. When a mapping is administratively disabled, the 5620 SAM raises no alarm in response to an associated trap from a GNE.

An alarm mapping can be static, which means that it maps to a specific alarm, or the mapping can use one or more transform functions that extend the mapping customization. A transform function defines conditions that enable the dynamic mapping of a trap to an alarm that is created using varbind values in an SNMP trap PDU. For example, you can use a transform function to assign a specific alarm name, severity, or probable cause to an alarm based on varbind values.

When the 5620 SAM receives a GNE trap that is not one of the supported standard traps or a mapped trap in an alarm catalog, the 5620 SAM drops the trap. When the 5620 SAM receives a high trap volume and must discard traps that it cannot process, it does not distinguish between standard and user-defined traps. To conserve system resources, Alcatel-Lucent recommends that you configure a GNE to send only the required traps to the 5620 SAM.

Traps that map to user-defined alarms require extra processing by the 5620 SAM and are managed in a separate, resource-limited queue. When this queue is full, the 5620 SAM discards some of the traps and raises an alarm. You can monitor the queue length using the 5620 SAM Resource Manager.

Note 1 — By default, only the 5620 SAM admin user, or an operator with an assigned admin scope of command role, can manage GNE profiles and alarm catalogs. A non-admin user requires the genericne scope of command role to manage GNE profiles.

Note 2 — To create, modify, or delete a GNE alarm catalog or mapping, you require a trapmapper scope of command role with write, update, and execute permissions.

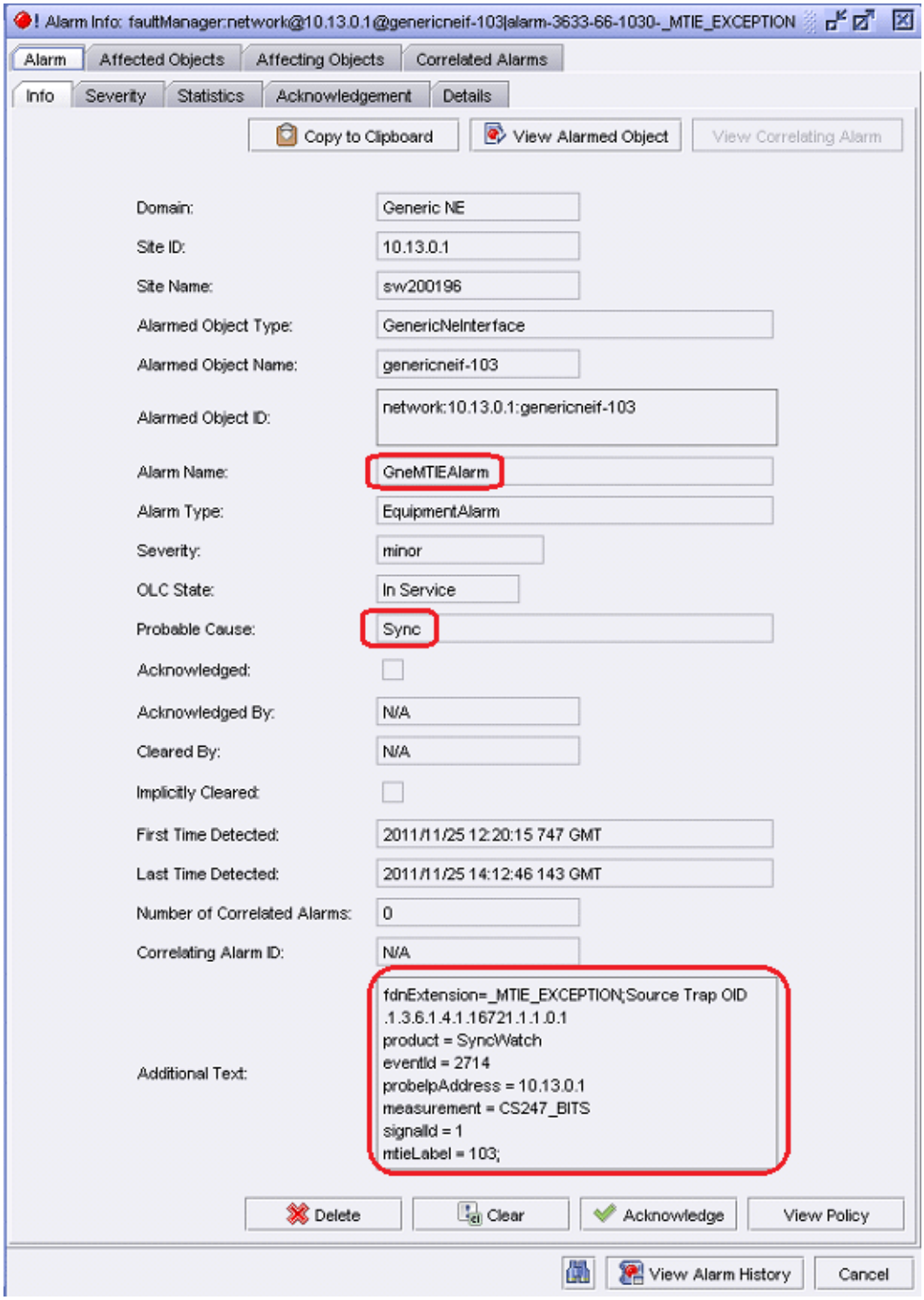
The 5620 SAM supports a system address and interface index in the alarm catalog such that the alarms are not always raised against the network element object associated with the GNE that sent the trap. Instead, the alarm can be raised:

- on a different GNE
- on an interface on the GNE, rather than only on the GNE

This index is necessary because the NetSMART Server sends traps on behalf of the SyncWatch Probes and because each probe has multiple interfaces.

Figure 5-1 shows a SyncWatch alarm displayed by the 5620 SAM.

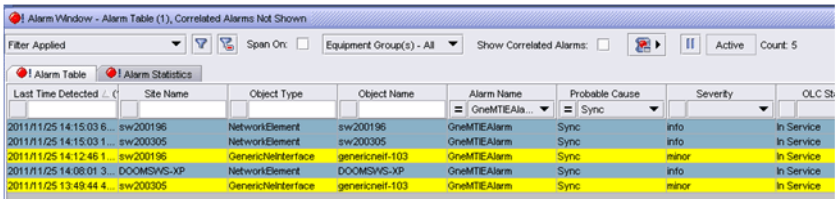
Figure 5-1 SyncWatch alarm in the 5620 SAM



You can view and monitor SyncWatch Probe alarms from several places on the 5620 SAM GUI.

- The topology map displays outstanding alarms in the top right corner of network icons. See Figure 5-11.
- The GNE properties form for the SyncWatch Probe displays GNE interfaces with outstanding alarms on the Generic NE Interfaces tab.
- The Generic NE Interface form lists alarms on the Faults tab.
- The Alarm Window displays a filterable list of network alarms. See Figure 5-2.

Figure 5-2 Alarm Window



You can view the Alarm Info form for a selected alarm to see details about the alarmed object and remedial actions. The additional text will depend on the configuration in the alarm catalog.

5.5 Equipment and software

Table 5-1 lists the equipment and software releases used to evaluate the configurations described in this document. This document applies primarily to these releases, because functionality may change in later releases.

Table 5-1 Applicable equipment and software releases

Application	Applicable release
5620 SAM	Release 9.0 R7 to 11.0 R1
NetSMART Server	Release 3.4 to 4.2
SyncWatch Probe	Release 3.4 to 4.2

5.6 Sample network

Table 5-2 lists the specifications for the network components that comprise the installation of the sample network described in this section.

Table 5-2 Sample network component specifications

Component	Specifications
NetSMART Server	"doomNSS" at 192.0.2.18 In-Band Mediation interface = 86.148.0.39
5620 SAM server 1	"sam1" at 192.0.2.242 In-Band Mediation interface = 86.148.0.33
5620 SAM server 2	"sam2" at 198.51.100.142 In-Band Mediation interface = 86.149.0.33

Figure 5-3 Management network

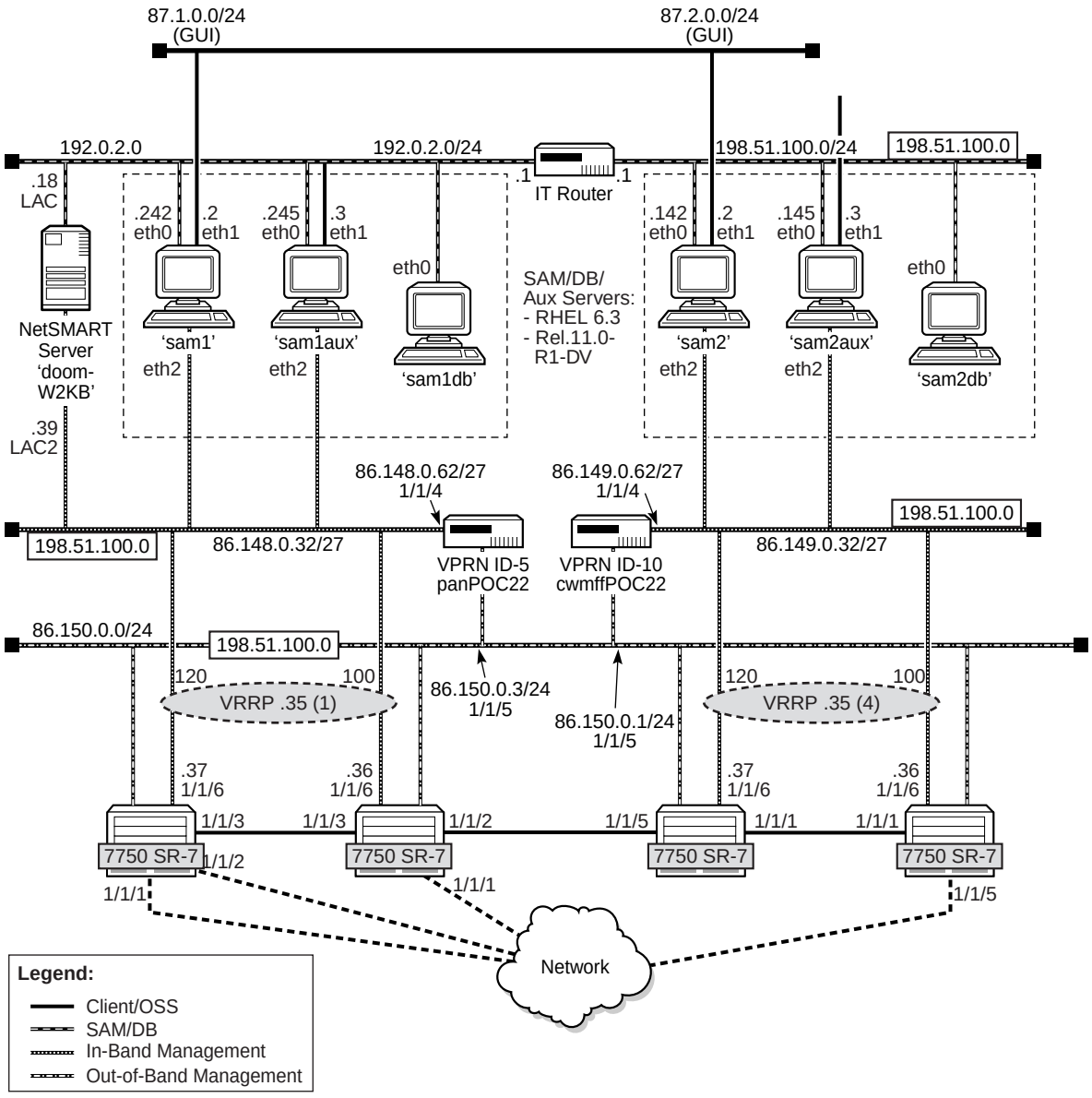
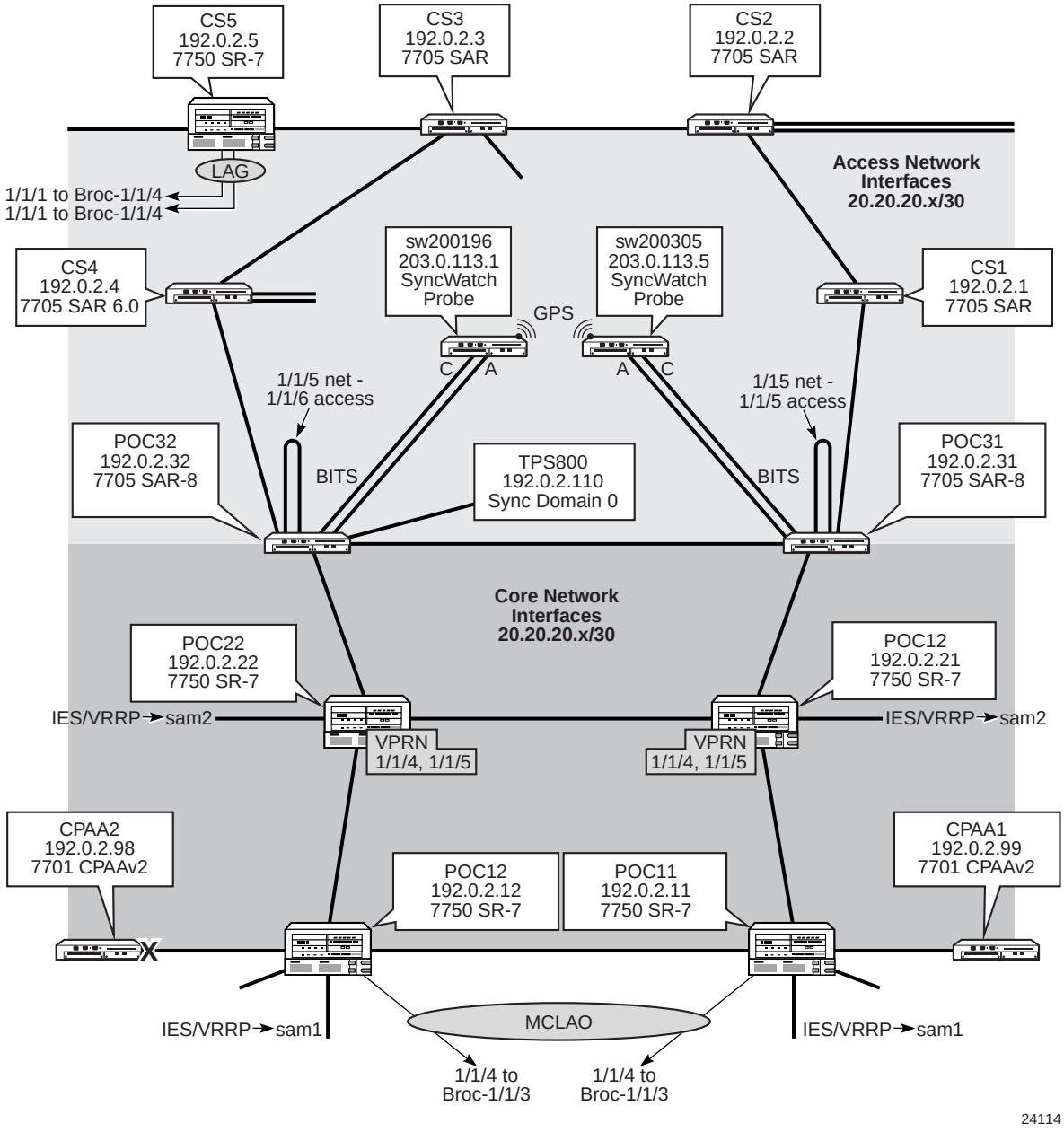


Figure 5-4 Mobile backhaul network with synchronization



5.7 Workflow for scripted SyncWatch integration

The following workflow describes the high-level steps that are required to execute the Chronos SyncWatch bundle for scripted integration with the 5620 SAM.

The procedures in this section assume that you have performed the following prerequisite tasks on the NetSMART Server.

- Verify the SNMP license. The Server Licences tab on the Server: Manage panel displays the SNMP license.
- Add users on the NetSMART Server. You can add new users from the Users: List panel. Ensure that all access rights are unchecked for the new users. A verification email is sent to new users with an automatically generated password.

Verify SNMP communications

1 Verify from a CLI session that the 5620 SAM can communicate with the NetSMART Server via SNMP. See Procedure 5-1.

2 Verify from a CLI session that the 5620 SAM can communicate with the SyncWatch Probes via SNMP. See Procedure 5-2.

Import and execute the Chronos SyncWatch script bundle

3 Import the script bundle into the 5620 SAM. See Procedure 5-3.

4 Execute the script bundle. The 5620 SAM prompts you for the server IP and user information. See Procedure 5-4.

Perform additional setup tasks

5 Perform a NetSMART Server cross-launch, as required. See Procedure 5-5.

6 The first physical link is configured by the script bundle to port C on the SyncWatch Probe. Other physical links need to be configured manually. Create additional physical links, as required. See Procedure 5-6.

5.8 Verify SNMP and user configurations

Perform the following procedures to verify that the NetSMART Server and SyncWatch Probe are configured for SNMP communication with the 5620 SAM.

Procedure 5-1 Verify 5620 SAM SNMP communications to the NetSMART Server

Perform this procedure to verify that the 5620 SAM can communicate with the NetSMART Server via SNMP. The 5620 SAM must be able to read the SNMPv2 sysDescr and derive the sysObjectID.

1 Open a console window.

2 Navigate to the SNMP configuration in the server binary directory:

```
bash# cd /opt/5620sam/server/nms/bin/unsupported/snmp
```

3 Obtain the SNMPv2 sysDescr:

```
bash# SnmpGet.bash -v 2 -h 172.20.148.20 -c public sysDescr

OID: .1.3.6.1.2.1.1.1.0 ->
```

```
NSS for SAM Integration
```

4 Verify that the 5620 SAM can derive the sysObjectID:

```
bash# SnmpGet.bash -v 2 -h 172.20.148.20 -c public sysObjectID
OID: .1.3.6.1.2.1.1.2.0 ->
.1.3.6.1.4.1.16721.1.3.1
```

Procedure 5-2 Verify 5620 SAM SNMP communications to the SyncWatch Probes

Perform this procedure to verify that the 5620 SAM can communicate with the SyncWatch Probes via SNMP. The 5620 SAM must be able to read the SNMPv2 sysDescr and derive the sysObjectID.

1 Open a console window.

2 Navigate to the SNMP configuration in the server binary directory:

```
bash# cd /opt/5620sam/server/nms/bin/unsupported/snmp
```

3 Obtain the SNMPv2 sysDescr:

```
bash# SnmpGet.bash -v 2 -h 10.13.0.1 -c public sysDescr
OID: .1.3.6.1.2.1.1.1.0 ->
Linux sw200196 2.6.21.3D #4 Fri Feb 26 17:16:47 GMT 2010armv5tejl
```

4 Verify that the 5620 SAM can derive the sysObjectID:

```
bash# SnmpGet.bash -v 2 -h 10.13.0.1 -c public sysObjectID
OID: .1.3.6.1.2.1.1.2.0 ->
.1.3.6.1.4.1.16721.1.3.2
```

5.9 Chronos SyncWatch script bundle execution

Perform these procedures to import and execute the Chronos SyncWatch script bundle. The script bundle performs the following setup operations:

- creates a SyncWatch alarm catalog
- creates a NetSMART Server GNE profile
- creates a NetSMART Server mediation profile
- creates and executes a NetSMART Server discovery rule
- creates a SyncWatch Probe GNE profile

- creates a SyncWatch Probe mediation profile
- creates a SyncWatch Probe discovery rule
- adds the SyncWatch Probe IP address to the probe discovery rule and discovers the probe
- creates a SyncWatch Probe GNE URL for the NetSMART Server cross-launch
- creates a physical link

See the *5620 SAM Scripts and Templates Developer Guide* for more information about script bundles and script management.

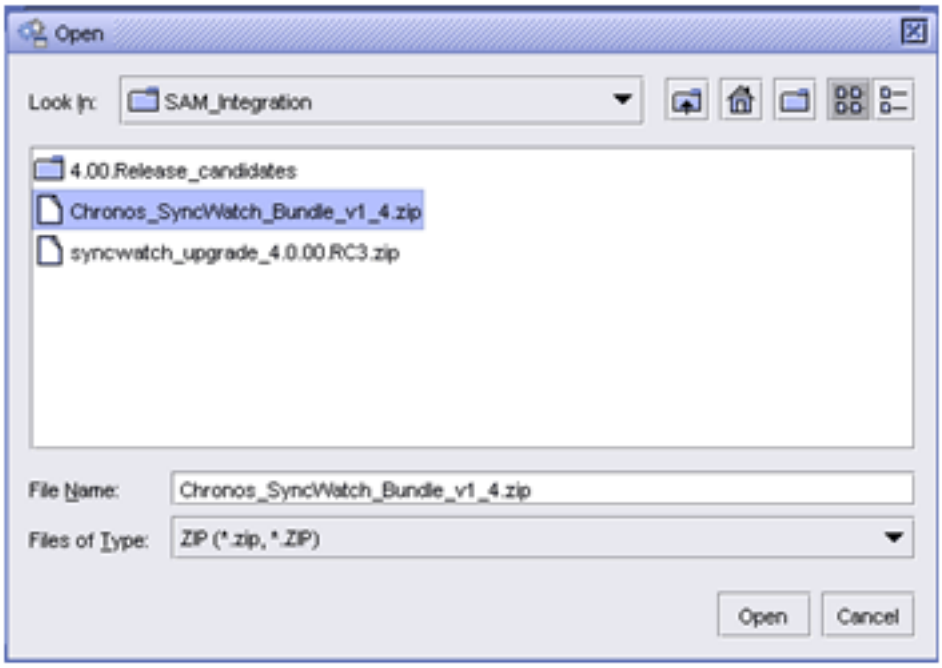
Procedure 5-3 To import the SyncWatch script bundle

1 Choose Tools→Scripts from the 5620 SAM main menu. The Scripts manager opens.

2 Click on the Import button. The Specify file to import form opens.

3 Navigate to the Chronos SyncWatch Bundle; see Figure 5-5.

Figure 5-5 SyncWatch script bundle



4 Click on the Open button. The Import form opens and lists the operations to be carried out.

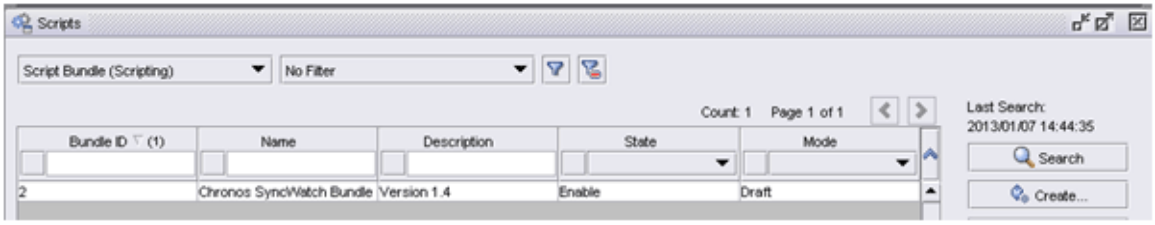
5 Click on the Continue button to execute the operations.

6 Click on the Close button when the operations are complete.

7 In the Scripts manager, choose Script Bundle (Scripting) from the object drop-down menu.

8 Search for the Chronos SyncWatch script bundle to confirm that it was successfully imported; see Figure 5-6.

Figure 5-6 Scripts manager



Procedure 5-4 To execute the SyncWatch script bundle

1 Choose Tools→Scripts from the 5620 SAM main menu. The Scripts manager opens.

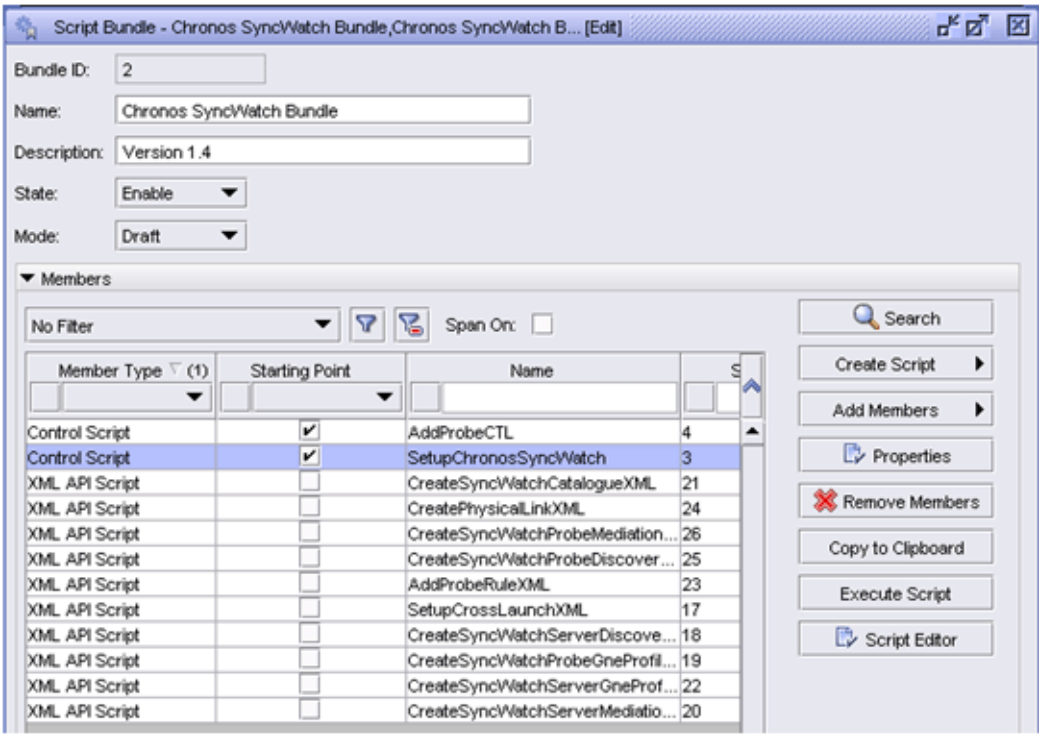
2 Choose Script Bundle (Scripting) from the object drop-down menu and search for the SyncWatch script bundle.

3 Select the script bundle and click on the Properties button. The Script Bundle (Edit) form opens; see Figure 5-7.

The Members tab displays the scripts included in the script bundle. The two control scripts are labeled as starting points for the bundle.

- SetupChronosSyncWatch — the starting point when adding the NetSMART Server
- AddProbeCTL — the starting point when adding the SyncWatch Probe

Figure 5-7 Chronos SyncWatch script bundle



4 Select the SetupChronosSyncWatch script and click on the Execute Script button. The Execute Script form opens with the Chronos SyncWatch tab displayed.

5 Configure the parameters:

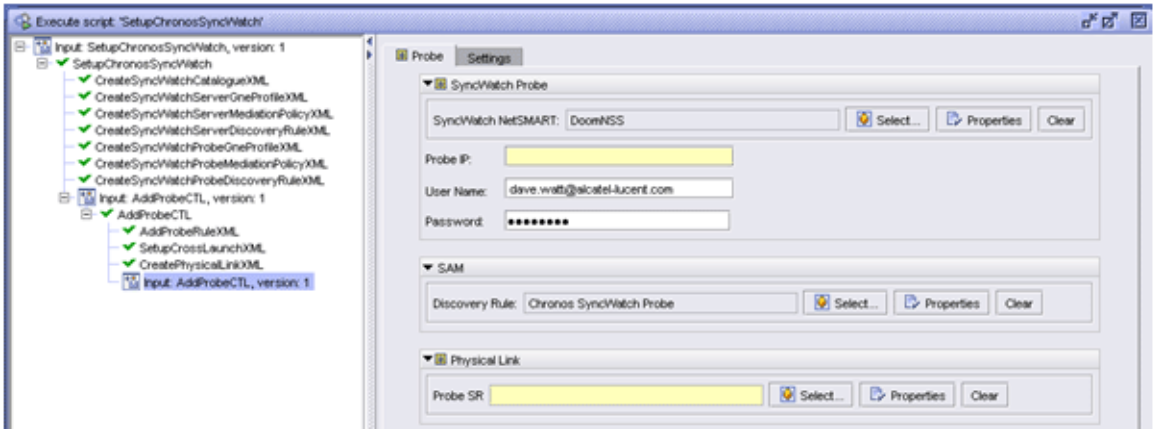
- NetSMART IP — enter the IP address corresponding to the trap receiving address of the 5620 SAM servers
- User Name
- Password — the username and password cannot be the same as the root user IP address corresponding to the trap receiving address of the 5620 SAM servers

6 Click on the Select button for the Group and select the equipment group into which the NetSMART Server is discovered.

7 Click on the Execute button. The component scripts are marked with green check marks when they are complete.

The Execute script form refreshes and prompts for information for the first SyncWatch Probe; see Figure 5-8.

Figure 5-8 Execute script form



8 Configure the parameters:

- Probe IP — enter the IP address by which the 5620 SAM communicates with the SyncWatch Probe
- User Name
- Password — the username and password are automatically populated from the NetSMART Server details configured in step 5.

9 Click on the Select button for the Probe SR and choose the node to which the first SyncWatch Probe measurement port is connected.

10 Click on the Execute button. The component scripts are marked with green check marks when they are complete.

11 Repeat steps 8 to 10 to configure parameters for additional SyncWatch Probes, as required.

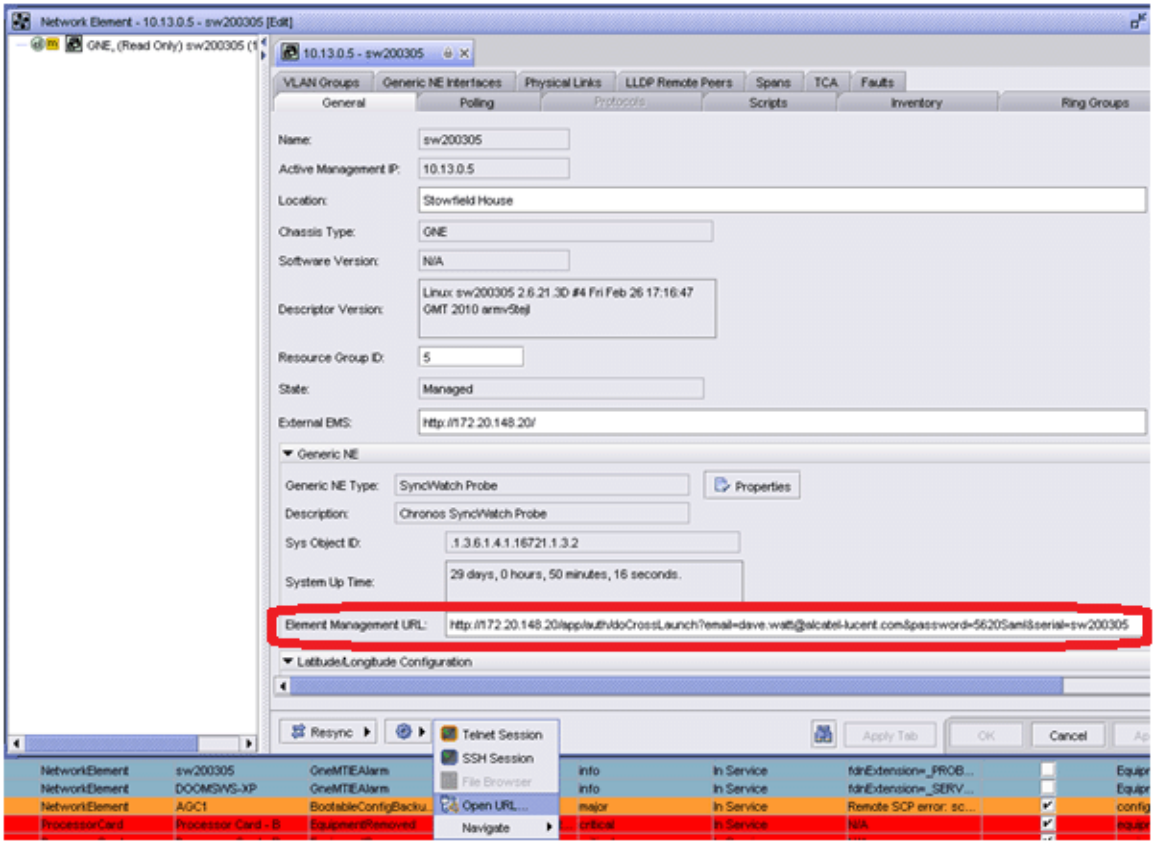
5.10 NetSMART Server cross-launch mechanism

You can execute a NetSMART Server cross-launch after you have configured an element management URL for the selected SyncWatch Probe.

Note — Only users with limited access rights can open a cross-launch session. This does not include the default root user.

You can configure the element management URL in the Network Element properties form for the selected SyncWatch Probe. Figure 5-9 shows the parameter.

Figure 5-9 Element management URL



Enter the URL using the following format:

```
http:// <SyncWatch_Server_IP> /app/auth/doCrossLaunch?email= <user>
&password= <password> &serial= <probe_serial_no>
```

- <SyncWatch_Server_IP> — IP (not resolvable host name) of NetSMART Server
- <user> <password> — NetSMART Server Username (Email) and password
- <probe_serial_no> — SyncWatch Probe serial number

Procedure 5-5 To perform a NetSMART Server cross-launch

1. Right-click on the SyncWatch Probe GNE icon on the topology map and choose Properties from the drop-down menu. The Network Element (Edit) form opens.
2. Configure the Element Management URL parameter using the format described in this section.
3. Click on the OK button to close the form.
4. Right-click on the SyncWatch Probe GNE icon on the topology map and choose Open URL. The cross-launch executes.

5.11 NetSMART Server and SyncWatch Probe in the 5620 SAM

This section describes how the NetSMART Server and SyncWatch Probe are managed in the 5620 SAM.

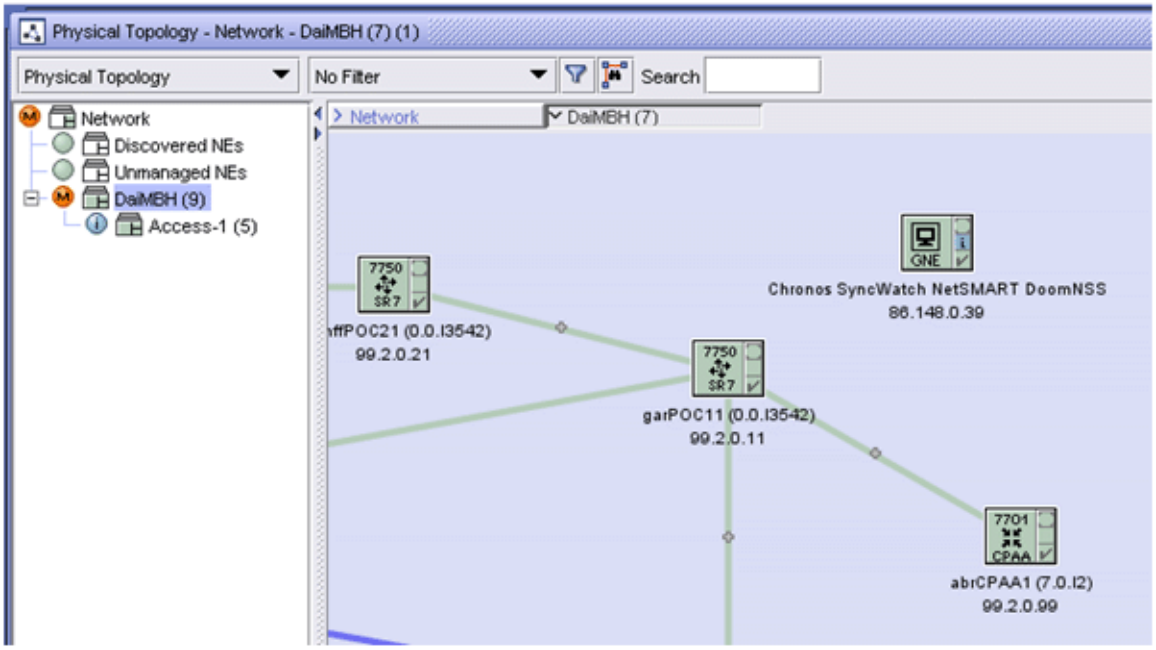
NetSMART Server

The 5620 SAM server scans through the list of rule elements within the discovery rule, of which there is only one in the case of the Chronos SyncWatch script bundle. Then, the 5620 SAM scans through the GNE profiles until it finds one that matches.

The NetSMART Server responds and the 5620 SAM populates its database with the required information from the MIB. An icon appears within the specified group on the topology map. You can right-click on the icon and choose Properties to view the read-only information in the properties form.

Figure 5-10 shows the NetSMART Server GNE icon as it appears on the topology map.

Figure 5-10 NetSMART Server on the 5620 SAM topology map



SyncWatch Probe

The 5620 SAM server scans through the list of rule elements within the SyncWatch Probe discovery rule, then scans through the GNE profiles until it finds one that matches.

The SyncWatch Probes respond and the 5620 SAM populates its database with the required information from the MIB. An icon will appears on within the chosen group on the topology map. You can right-click on the icon and choose Properties to view read-only probe and interface information on the properties form.

Note — If the auto-generated string for the Element Management URL in the SyncWatch Probe properties form displays a different IP address from that accessible by the 5620 SAM, you must reconfigure it. This mismatch occurs typically in a multi-LAN topology. The URL string may display the in-band management interface for the NetSMART Server. For cross-launch, the 5620 SAM has access only to the GUI interface.

SyncWatch Probe physical links

The first measurement is configured by the script bundle to port C on the SyncWatch Probe. Other measurement links need to be configured manually because LLDP is not supported on the SyncWatch Probe and currently the 7x50 synchronization outputs are not modeled on the nodes or the 5620 SAM.

Procedure 5-6 To configure a physical link

1 Right-click on the topology map and choose Equipment→Create Physical Link from the drop-down menu. The Physical Link (Create) form opens.

2 Perform one of the following:

   a Configure a link representing the GPS reference input.

      i Configure the parameters:

         - Name
         - Description
         - Endpoint A Type — choose Generic NE Interface
         - Endpoint B Type — choose Unmanaged NE
         - Notes

ii Click on the Select button for Endpoint A to specify the GNE interface.

iii Configure the parameters:

- Unmanaged — Name
- Unmanaged Management Address — enter 0.0.0.0
- Unmanaged Description

b Configure a link representing the SAR BITS output to the SyncWatch Probe measurement input.

i Configure the parameters:

- Name
- Description
- Endpoint A Type — choose Generic NE Interface
- Endpoint B Type — choose Network Element
- Notes

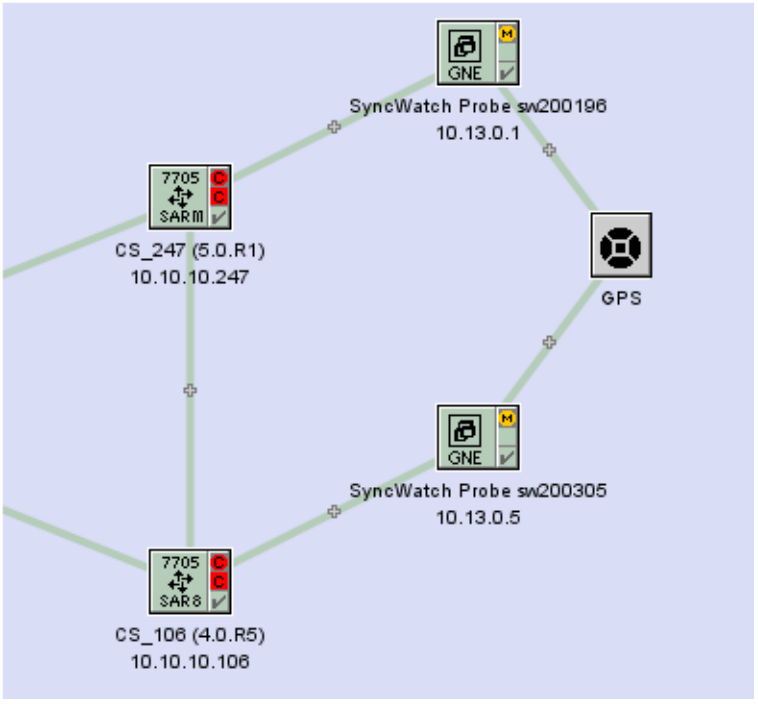
ii Click on the Select button for Endpoint A to specify the GNE interface.

iii Click on the Select button for Endpoint B to specify the NE interface.

3 Click on the OK button to create the physical link.

Figure 5-11 shows the updated topology map.

Figure 5-11 Topology map with physical link



5.12 Workflow for manual SyncWatch integration

The following workflow describes the high-level steps that are required to manually configure SyncWatch integration with the 5620 SAM. This workflow may be applicable if the script bundle fails to execute, or if you want to configure parts of the setup process manually.

The procedures in this section assume that you have performed the following prerequisite tasks on the NetSMART Server.

- Verify the SNMP license. The Server Licences tab on the Server: Manage panel displays the SNMP license.
- Add users on the NetSMART Server. You can add new users from the Users: List panel. Ensure that all access rights are unchecked for the new users. A verification email is sent to new users with an automatically generated password.

Verify SNMP communications

1 Verify from a CLI session that the 5620 SAM can communicate with the NetSMART Server. See Procedure 5-1.

2 Verify from a CLI session that the 5620 SAM can communicate with the SyncWatch Probes. See Procedure 5-2.

Note — Section 5.13 describes the configuration tasks in workflow steps 3 to 12.

Create GNE profile components for the NetSMART Server

3 Create an alarm catalog for the NetSMART Server. You must define raising alarm mappings and transform functions for traps imported from the NetSMART Server.

4 Create a GNE profile for the NetSMART Server. You must assign the alarm catalog created in step 3.

5 Create a mediation policy for the NetSMART Server.

6 Create and execute a discovery rule for the NetSMART Server. You must select the mediation policy created in step 5.

Create GNE profile components for the SyncWatch Probes

7 Create a GNE profile for the SyncWatch Probes. You must create three interface types.

8 Create a mediation policy for the SyncWatch Probes.

9 Create and execute a discovery rule for the SyncWatch Probes. You must select the mediation policy created in step 8.

Perform additional setup tasks

10 Define a NetSMART Server cross-launch URL. You should enter the URL in a specific format defined in section 5.10.

11 Perform a NetSMART Server cross-launch, as required. See Procedure 5-5.

12 Create physical links between the SyncWatch Probe and any managed NEs. See Procedure 5-6.

5.13 Manual SyncWatch Probe integration

Section 5.7 describes how to discover and configure the SyncWatch Probes and NetSMART Server using an automated script bundle. This section describes how to perform the script functions manually. These instructions may be useful if the script bundle fails or if you prefer to configure certain components manually.

See the *5620 SAM User Guide* for more generalized descriptions and procedures about GNE integration. The sample described in Table 5-3 is specific to SyncWatch Probe and NetSMART Server discovery and integration.

Configuration forms for GNE alarm catalogs, GNE profiles, mediation policies, and discovery rules can be accessed from the Administration menu on the 5620 SAM GUI.

Table 5-3 SyncWatch Probe integration

Task	Description

1. Create a GNE alarm catalog for the NetSMART Server	• Create a GNE alarm catalog and configure a name and description.
	• Create raising alarm mappings. Mappings are required to interpret the various SNMP traps that are issued by the NetSMART Server.
	  • The System Address Varbind Position parameter allows the trap from the NetSMART Server to generate a 5620 SAM alarm for the appropriate SyncWatch Probe.
	  • The Interface Index Varbind Position parameter allows the trap from the NetSMART Server to generate a 5620 SAM alarm for the appropriate SyncWatch Probe interface.
	• Create transform functions. Transform functions are required to define the raising and clearing alarm pairs.

2. Create a GNE profile for the NetSMART Server	• Create a GNE profile.
	• Select Server for the Generic NE Category parameter.
	• Enter the sysObjectID derived in Procedure 5-1 for the Sys Object ID parameter.
	• Enter the NetSMART Server URL for the Default Element Manager URL parameter.
	  • This step allows you to open the NetSMART Server from the 5620 SAM GUI.
	• Assign the alarm catalog created in the previous task to the GNE profile.
	• Complete the GNE profile creation.
	  • The CLI Profile tab is dimmed because CLI is not supported for the NetSMART Server.
	  • Do not configure the trap configuration scripts because trap configuration is handled from the NetSMART Server.
	  • Do not add interface types because the NetSMART Server MIB does not include interface information.

3. Create a mediation policy for the NetSMART Server	• From the Mediation (Edit) form, click on the Mediation Security tab and create a mediation policy. • Select SNMPv2c for the Security Model parameter. • Enter “public” for the SNMP v1/v2c Community String parameter. • Do not configure CLI or file transfer access because they are not accessible.

(1 of 2)

Task	Description
4. Create a discovery rule for the NetSMART Server	• Create a discovery rule. • In step 1 of discovery rule creation, select a group into which the NetSMART Sever is discovered. • In step 2 of discovery rule creation, add the NetSMART Server IP address with a 32-bit mask. • Do not configure ACL in step 3 of discovery rule creation. • In step 4 of discovery rule creation, select the mediation policy created in the previous task for the read access, write access, and trap access mediation policies. • Do not perform other steps. Complete the discovery rule creation.

5. Create a GNE profile for the SyncWatch Probes	• Create a GNE profile.
	• Select GNE1 for the Generic NE Category parameter.
	• Enter the sysObjectID derived in Procedure 5-2 for the Sys Object ID parameter.
	• Enter the SyncWatch Probe element management URL for the Default Element Manager URL parameter.
	  • See section 5.10 for information about the URL format.
	• Create the following interface types:
	  • 1 — Other
	  • 6 — Ethernet Csmacd
	  • 24 — Software Loopback
	• Complete the GNE profile creation.
	  • The CLI Profile tab is dimmed because CLI is not supported for the SyncWatch Probe.
	  • Do not configure the trap configuration scripts because trap configuration is handled from the NetSMART Server.

6. Create a mediation policy for the SyncWatch Probes	• From the Mediation (Edit) form, click on the Mediation Security tab and create a mediation policy. • Select SNMPv2c for the Security Model parameter. • Enter “public” for the SNMP v1/v2c Community String parameter. • Do not configure CLI or file transfer access, as they are not accessible.
7. Create a discovery rule for the SyncWatch Probes	• Create a discovery rule. • In step 1 of discovery rule creation, select a group into which the NetSMART Sever is discovered. • In step 2 of discovery rule creation, add the SyncWatch Probe IP addresses with a 32-bit mask. • Do not configure ACL in step 3 of discovery rule creation. • In step 4 of discovery rule creation, select the mediation policy created in the previous task for the read access, write access, and trap access mediation policies. • Do not perform other steps. Complete discovery rule creation.
8. Define a NetSMART Server cross-launch URL	See section 5.10 for information about configuring the URL NetSMART Server cross-launch URL.
9. Create physical links between the SyncWatch Probes and a managed NE	See Procedure 5-6 for information about configuring a physical link.

(2 of 2)

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