NOKIA

5620 SAM
SERVICE AWARE MANAGER

14.0 R12

Integration Guide

3HE-10689-AAAK-TQZZA

Issue 1

July 2019

Legal notice

Contents

About this document

Purpose

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.

The *5620 SAM Integration Guide* contains information about integrating the 5620 SAM with third-party and Nokia systems to enable additional functions.

Safety information

For your safety, this document contains safety statements. Safety statements are given at points where risks of damage to personnel, equipment, and operation may exist. Failure to follow the directions in a safety statement may result in serious consequences.

Document support

Customer documentation and product support URLs:

Customer documentation welcome page

- https://infoproducts.nokia.com/cgi-bin/doc_welc.pl

Technical support

- http://support.nokia.com

How to comment

Documentation feedback

- documentation.feedback@nokia.com

1 Safety information

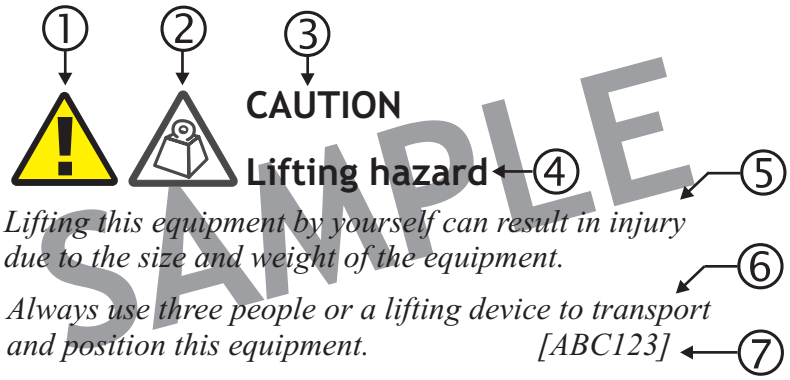
1.1 Structure of safety statements

1.1.1 Overview

This topic describes the components of safety statements that appear in this document.

1.1.2 General structure

Safety statements include the following structural elements:



Item	Structure element	Purpose
1	Safety alert symbol	Indicates the potential for personal injury (optional)
2	Safety symbol	Indicates hazard type (optional)
3	Signal word	Indicates the severity of the hazard
4	Hazard type	Describes the source of the risk of damage or injury
5	Safety message	Consequences if protective measures fail
6	Avoidance message	Protective measures to take to avoid the hazard
7	Identifier	The reference ID of the safety statement (optional)

1.1.3 Signal words

The signal words identify the hazard severity levels as follows:

Signal word	Meaning
DANGER	Indicates an extremely hazardous situation which, if not avoided, will result in death or serious injury.
WARNING	Indicates a hazardous situation which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a hazardous situation not related to personal injury.

2 5620 SAM integration overview

2.1 Overview

2.1.1 Purpose

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.

2.1.2 Contents

2.2 Integration overview

2.2.1 Integration with other systems

The *5620 SAM Integration Guide* contains information about integrating the 5620 SAM with third-party and Nokia systems to enable additional functions.

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 3, “5620 SAM integration with other systems” for more information.

2.2.2 Integration with Single Sign On

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

See Chapter 4, “5620 SAM integration with Single Sign On” for more information.

2.2.3 Integration with Chronos SyncWatch

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

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

See Chapter 5, “5620 SAM integration with Chronos SyncWatch” for more information.

3 5620 SAM integration with other systems

3.1 Overview

3.1.1 Purpose

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.

3.1.2 Contents

5620 SAM and 5650 CPAM integration

3.2 5620 SAM and 5650 CPAM integration

3.2.1 General Information

The 5650 CPAM provides real-time control-plane IGP and BGP topology capture, inspection, visualization, and troubleshooting. The 5650 CPAM product is bundled with the 5620 SAM product; this 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. The 5650 CPAM has access to the 5620 SAM managed objects and displays the objects in 5650 CPAM topology views.

The 5650 CPAM provides a real-time view of the network, including routing topology and associated configurations performed by GUI or OSS clients, or using a CLI. The 5650 CPAM facilitates navigation between protocol maps and managed objects, such as protocol links.

The 5650 CPAM functions are enabled by default, and are available from the 5620 SAM main menu. See the 5650 CPAM User Guide for information about using a function.

5620 SAM and other systems integration

3.3 5620 SAM and EM systems integration

3.3.1 General Information

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.

3.4 5620 SAM and 5670 RAM integration

3.4.1 General Information

The 5670 RAM server processes AA statistics. The 5620 SAM statistics collector, which is a main or auxiliary 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 Installation and Upgrade Guide* for information about enabling 5620 SAM AA statistics collection.

See the 5620 SAM User Guide for information about AA.

3.5 To enable 5670 RAM support

3.5.1 Purpose

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

3.5.2 Steps

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 /opt/5620sam/server/nms/config directory.

4

Create a backup copy of the nms-server.xml file.

5

CAUTION

Service Disruption

Contact your Nokia 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.

Open the nms-server.fml file using a plain-text editor.

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 /opt/5620sam/server/nms/bin directory.

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 Step 2 to Step 12 on the standby main server.

14

Close the open console windows.

END OF STEPS

3.6 5620 SAM and DSC integration

3.6.1 General Information

The 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 DSC. The 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 DSC discovery and management using the 5620 SAM.

3.7 5620 SAM and 5520 AMS integration

3.7.1 General Information

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. These alarms are then correlated and shown against the corresponding network element within the 5620 SAM client GUI.

4 5620 SAM integration with Single Sign On

4.1 Overview

4.1.1 Purpose

Single Sign On, or SSO, enables user access to all resources in a domain after having entered their credentials 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 multiple prompts.

Users who access the 5620 SAM client GUI through Internet Explorer must deselect the “Do not save encrypted pages to disk” security option. The SANE Client for SSO is only supported in a Windows environment.

Use the following procedures to enable 5620 SAM SSO integration.

4.1.2 Contents

4.2 To configure 5620 SAM and SANE portal integration

4.2.1 Purpose

Perform this procedure to enable 5620 SAM system integration with the SANE portal.

Note: The SANE Client for SSO is only supported in a Windows environment.

CAUTION

Service Disruption

Enabling 5620 SAM and SANE portal integration requires a restart of each 5620 SAM main server, which causes a network management outage.

Ensure that you perform the 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 — network management outage begins
- server activity switch completes — network management outage ends
- primary main server reconfigured
- primary main server started
- if required, manual activity switch performed to restore initial main server roles

4.2.2 Before you begin

Note: You require the following user privileges on each main server station:

- root
- samadmin

Note: 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: You must perform this procedure on each main server in the 5620 SAM system . In a redundant system, you must perform the procedure on the standby main server first.

4.2.3 Steps

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 Installation and Upgrade Guide* up to, but not including, the step that describes opening the samconfig utility.

b. If you are configuring SANE access on an installed main server, stop the main server if it is running.

1. Log in to the main server station as the samadmin user.
2. Open a console window.

3. Enter the following:

   ```
   bash$ cd /opt/5620sam/server/nms/bin ↲
   ```

4. Enter the following:

   ```
   bash$ ./nmsserver.bash stop ↲
   ```

5. Enter the following to display the 5620 SAM main server status:

   ```
   bash$ ./nmsserver.bash appserver_status ↲
   ```

   The command displays a status message.

6. The main server is stopped when the command displays the following:

   ```
   Application Server is stopped
   ```

   If the command displays a different message, wait five minutes and repeat Step 1 b 5. Do not proceed until the server is stopped.

7. Enter the following to switch to the root user:

   ```
   bash$ su - ↲
   ```

2

Enter the following:

```
# samconfig -m main -sane ↲
```

The following is displayed:

```
Start processing command line inputs...
<main>
```

3

Enter the following:

```
<main> configure ssl secure ↲
```

The prompt changes to `<main configure>`.

4

Enter the following:

```
<main configure ssl> keystore-file file ↲
```

where *file* is the absolute path of the SSL keystore file on the main server

5

Enter the following:

```
<main configure ssl> keystore-pass password ↲
```

where *password* is the SSL keystore password

6

Enter the following:

```
<main configure ssl> truststore-file file ↲
```

where *file* is the absolute path of the SSL truststore file on the main server

7

Enter the following:

```
<main configure ssl> truststore-pass password ↵
```

where *password* is the SSL truststore password

8

Enter the following:

```
<main configure ssl> back ↵
```

The prompt changes to <main configure>.

9

Enter the following:

```
<main configure> sane hostname hostname ↵
```

where *hostname* is the main server hostname

The prompt changes to <main configure sane>.

10

Enter the following:

```
<main configure sane> windows-dir directory ↵
```

where *directory* is the absolute path of the GUI client installation location on Windows client stations

11

Enter the following:

```
<main configure sane> linux-dir directory ↵
```

where *directory* is the absolute path of the GUI client installation location on RHEL client stations

12

Enter the following:

```
<main configure sane> certificates certificate-list ↵
```

where *certificate-list* is a list of paired entities and certificate file paths in the following format:

entity1#path1;entity2#path2...entityn#pathn

13

Enter the following:

```
<main configure sane> back ↵
```

The prompt changes to <main configure>.

14

Perform one of the following.

a. If you are configuring SANE access during a main server installation or upgrade, perform the remaining installation or upgrade procedure steps.

b. If you are configuring SANE access on an installed main server, perform the following steps.

1. Enter the following:

   <main configure> **back** ↵

   The prompt changes to <main>.

2. Enter the following:

   <main> **apply** ↵

   The configuration is applied.

3. Enter the following:

   <main> **exit** ↵

   The samconfig utility closes.

4. Enter the following to switch back to the samadmin user:

   # **exit** ↵

5. 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.

6. If required, in a redundant deployment, after SANE access is configured on the primary main server, perform a manual server activity switch to restore the initial primary and standby main server roles.

END OF STEPS

5 5620 SAM integration with Chronos SyncWatch

5.1 Overview

5.1.1 Purpose

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.

5.1.2 Contents

5.2 Synchronization overview

5.2.1 General Information

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.

5.2.2 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.

5.2.3 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.

5.2.4 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.

5.2.5 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.

5.2.6 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

5.3.1 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.

5.3.2 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, Nokia 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: 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.

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.

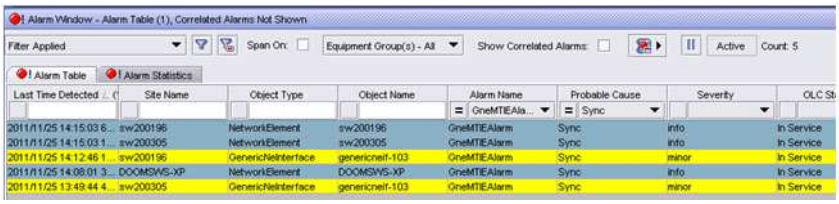
The following figure shows a SyncWatch alarm displayed by the 5620 SAM.

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 5-7, “Topology map with physical link” (p. 42) .
- 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, “Alarm Window” (p. 27) .

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.

5.3.3 Platform and software requirements

See the Chronos SyncWatch documentation for the NetSmart Server and SyncWatch Probe platform requirements. Consult Nokia technical support for information about SynchWatch and 5620 SAM release compatibility.

5.4 NetSMART Server and SyncWatch Probe in the 5620 SAM

5.4.1 General Information

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

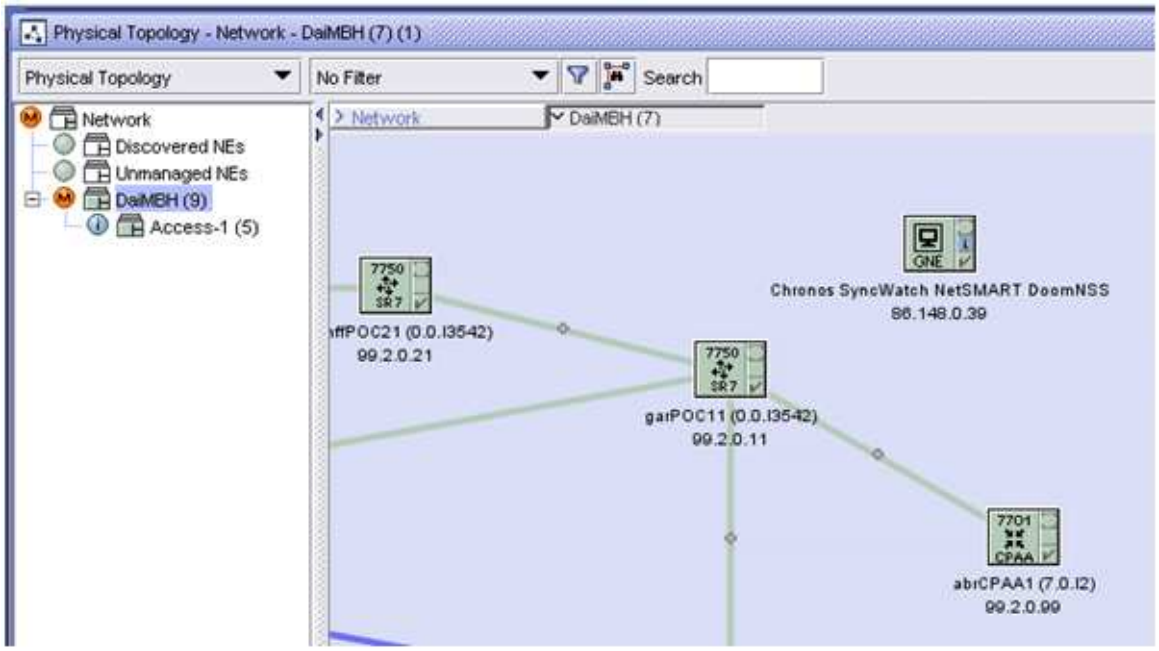
5.4.2 NetSMART Server

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.

The following figure shows the NetSMART Server GNE icon as it appears on the topology map.

Figure 5-3 NetSMART Server on the 5620 SAM topology map



5.4.3 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. Such a mismatch typically occurs in a multi-LAN topology. The URL string may contain 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.

5.5 Sample network

5.5.1 Components

Table 5-1 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 5-4 Management network

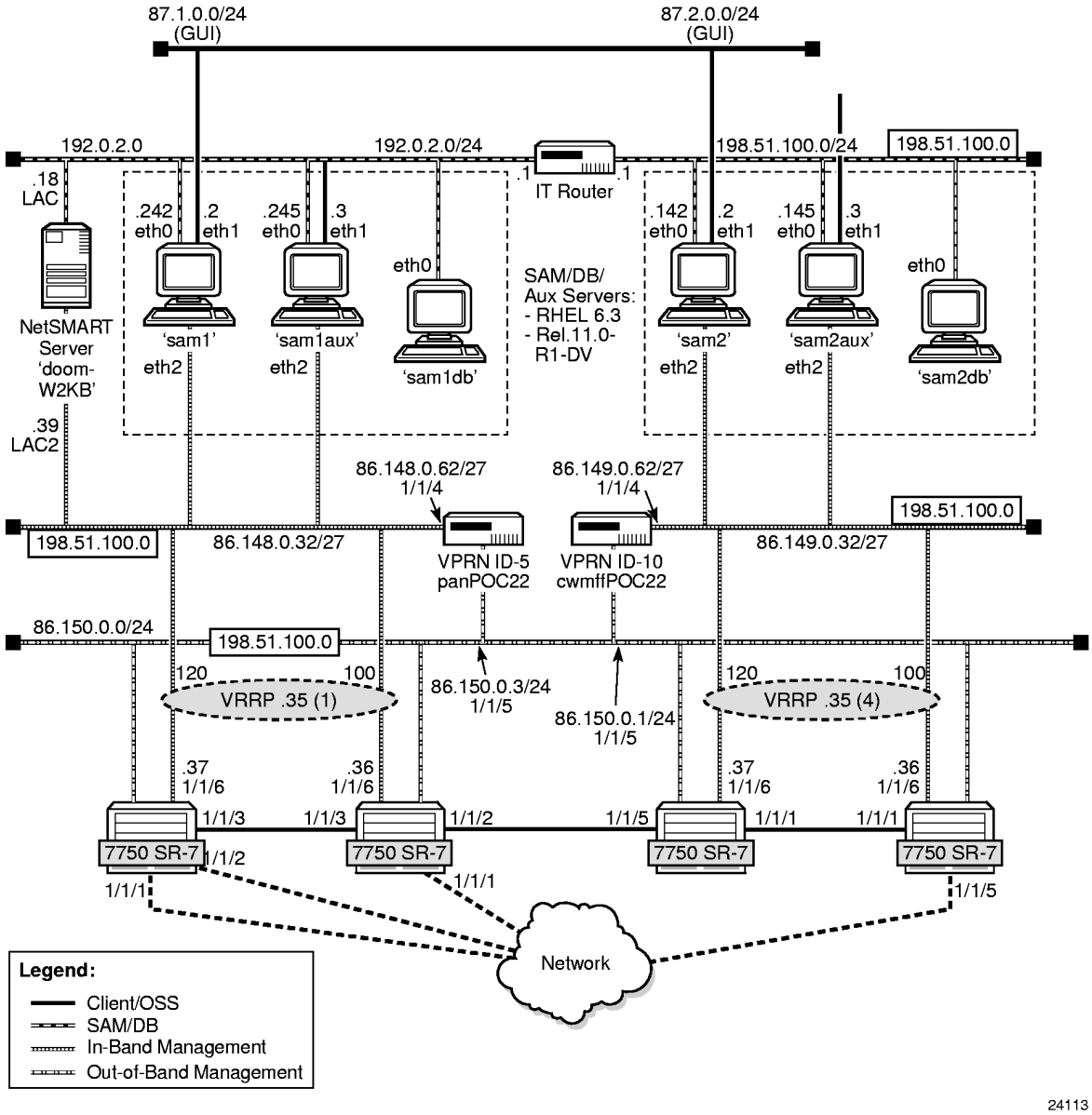
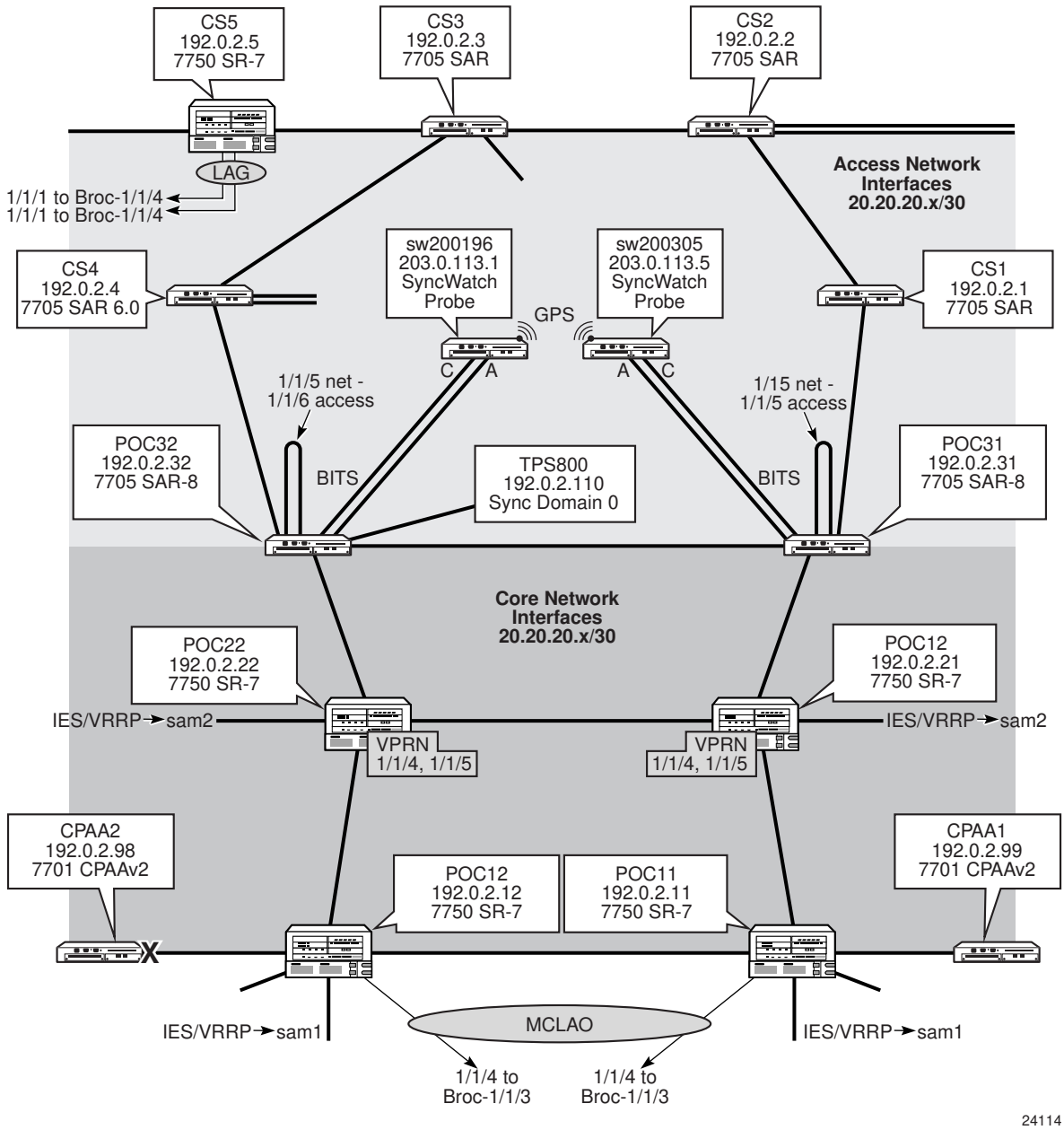


Figure 5-5 Mobile backhaul network with synchronization



5.6 Workflow for scripted SyncWatch integration

5.6.1 General Information

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.

5.6.2 Process

Verify SNMP communication

1

Verify from a CLI session that the 5620 SAM can communicate with the NetSMART Server via SNMP. See 5.9 “Verify 5620 SAM SNMP communication with NetSMART Server” (p. 38) .

2

Verify from a CLI session that the 5620 SAM can communicate with the SyncWatch Probes via SNMP. See 5.10 “Verify 5620 SAM SNMP communication with SyncWatch Probes” (p. 39) .

Import and execute the Chronos SyncWatch script bundle

3

Import the script bundle into the 5620 SAM. See 5.14 “To import the SyncWatch script bundle” (p. 43) .

4

Execute the script bundle. The 5620 SAM prompts you for the server IP and user information. See 5.15 “To execute the SyncWatch script bundle” (p. 45) .

Perform additional setup tasks

5

Perform a NetSMART Server cross-launch, as required. See 5.11 “To perform a NetSMART Server cross-launch” (p. 40) .

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 .

5.7 Workflow for manual SyncWatch integration

5.7.1 Overview

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.

5.7.2 Process

Verify SNMP communications

1

Verify from a CLI session that the 5620 SAM can communicate with the NetSMART Server. See 5.9 “Verify 5620 SAM SNMP communication with NetSMART Server” (p. 38) .

2

Verify from a CLI session that the 5620 SAM can communicate with the SyncWatch Probes. See 5.10 “Verify 5620 SAM SNMP communication with SyncWatch Probes” (p. 39) .

Note: 5.8 “Manual SyncWatch Probe integration” (p. 35) describes the configuration tasks in workflow Stage 3 to Stage 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 Stage 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 Stage 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 Stage 8 .

Perform additional setup tasks

10

Define a NetSMART Server cross-launch URL. You should enter the URL in a specific format defined in 5.11.1 “NetSMART Server cross-launch mechanism” (p. 40) .

11

Perform a NetSMART Server cross-launch, as required. See 5.11 “To perform a NetSMART Server cross-launch” (p. 40) .

12

Create physical links between the SyncWatch Probe and any managed NEs. See .

5.8 Manual SyncWatch Probe integration

5.8.1 Overview

5.6 “Workflow for scripted SyncWatch integration” (p. 33) 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 5-2, “SyncWatch Probe integration” (p. 36) 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 5-2 SyncWatch Probe integration

Task	Description
1. Create a GNE alarm catalog for the NetSMART Server	Tasks: • 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	Tasks: • Create a GNE profile. • Select Server for the Generic NE Category parameter. • Enter the sysObjectID derived in 5.9 “Verify 5620 SAM SNMP communication with NetSMART Server” (p. 38) 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.

Table 5-2 SyncWatch Probe integration (continued)

Task	Description
3. Create a mediation policy for the NetSMART Server	Tasks: • 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.
4. Create a discovery rule for the NetSMART Server	Tasks: • 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	Tasks: • Create a GNE profile. • Select GNE1 for the Generic NE Category parameter. • Enter the sysObjectID derived in 5.10 “Verify 5620 SAM SNMP communication with SyncWatch Probes” (p. 39) for the Sys Object ID parameter. • Enter the SyncWatch Probe element management URL for the Default Element Manager URL parameter. - See 5.11.1 “NetSMART Server cross-launch mechanism” (p. 40) 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.

Table 5-2 SyncWatch Probe integration (continued)

Task	Description
6. Create a mediation policy for the SyncWatch Probes	Tasks: • 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	Tasks: • 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 5.11.1 “NetSMART Server cross-launch mechanism” (p. 40) for information about configuring the URL NetSMART Server cross-launch URL.
9. Create physical links between the SyncWatch Probes and a managed NE	See 5.12 “To configure a physical link” (p. 41) for information about configuring a physical link.

5.9 Verify 5620 SAM SNMP communication with NetSMART Server

5.9.1 Purpose

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.

5.9.2 Steps

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
```

END OF STEPS

5.10 Verify 5620 SAM SNMP communication with SyncWatch Probes

5.10.1 Purpose

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.

5.10.2 Steps

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
```

END OF STEPS

5.11 To perform a NetSMART Server cross-launch

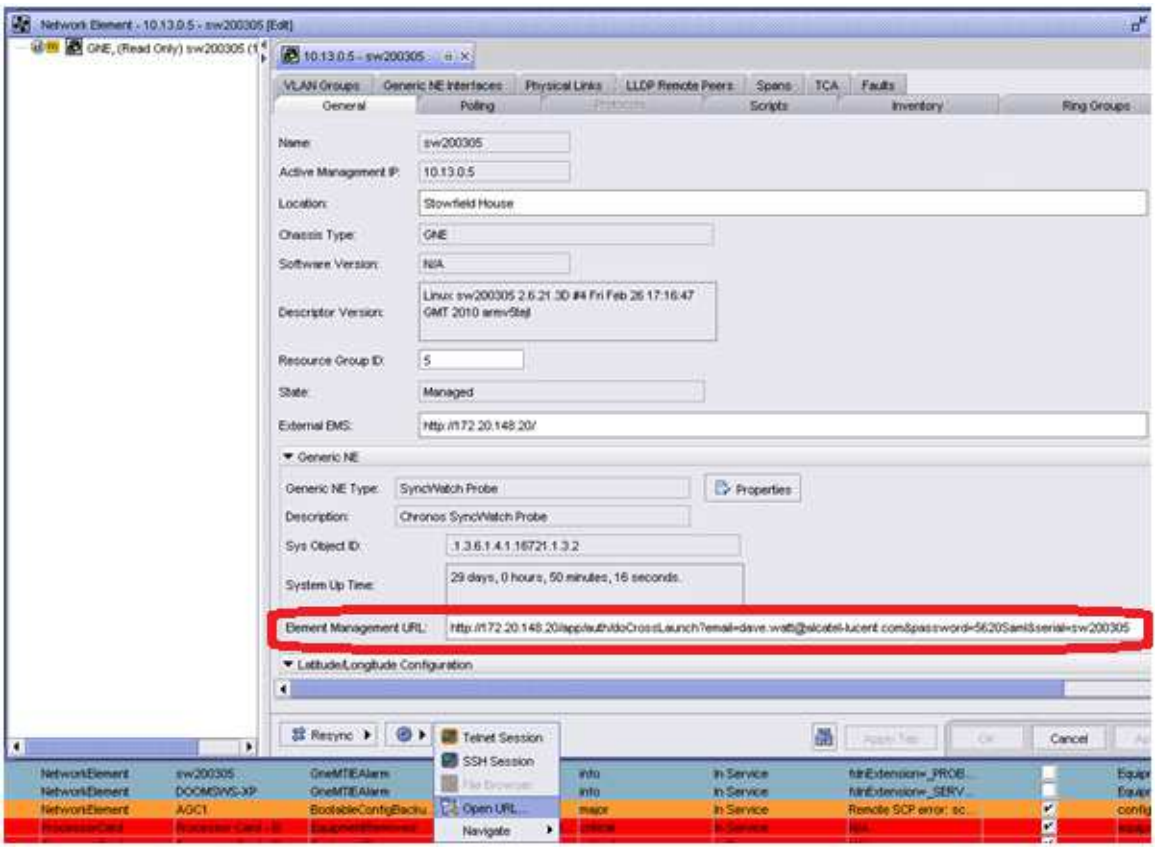
5.11.1 NetSMART Server cross-launch mechanism

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. The following figure shows the parameter.

Figure 5-6 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>
```

Where:

- <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

5.11.2 Steps

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.

END OF STEPS

5.12 To configure a physical link

5.12.1 Steps

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.

1. Configure the parameters:
   - Name
   - Description
   - Endpoint A Type — choose Generic NE Interface

- Endpoint B Type — choose Unmanaged NE
- Notes

2. Click on the Select button for Endpoint A to specify the GNE interface.
3. Configure the parameters:
   - Unmanaged — Name
   - Unmanaged Management Address — enter 0.0.0.0
   - Unmanaged Description

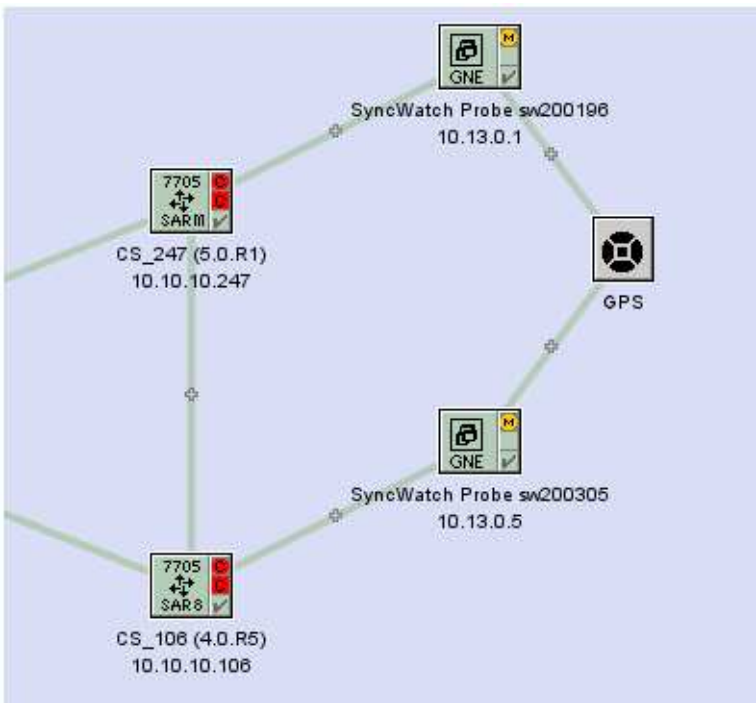
b. Configure a link representing the SAR BITS output to the SyncWatch Probe measurement input.

1. Configure the parameters:
   - Name
   - Description
   - Endpoint A Type — choose Generic NE Interface
   - Endpoint B Type — choose Network Element
   - Notes
2. Click on the Select button for Endpoint A to specify the GNE interface.
3. 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 5-7 Topology map with physical link



END OF STEPS

5.13 Chronos SyncWatch script bundle execution

5.13.1 General Information

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.

5.14 To import the SyncWatch script bundle

5.14.1 Steps

1

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

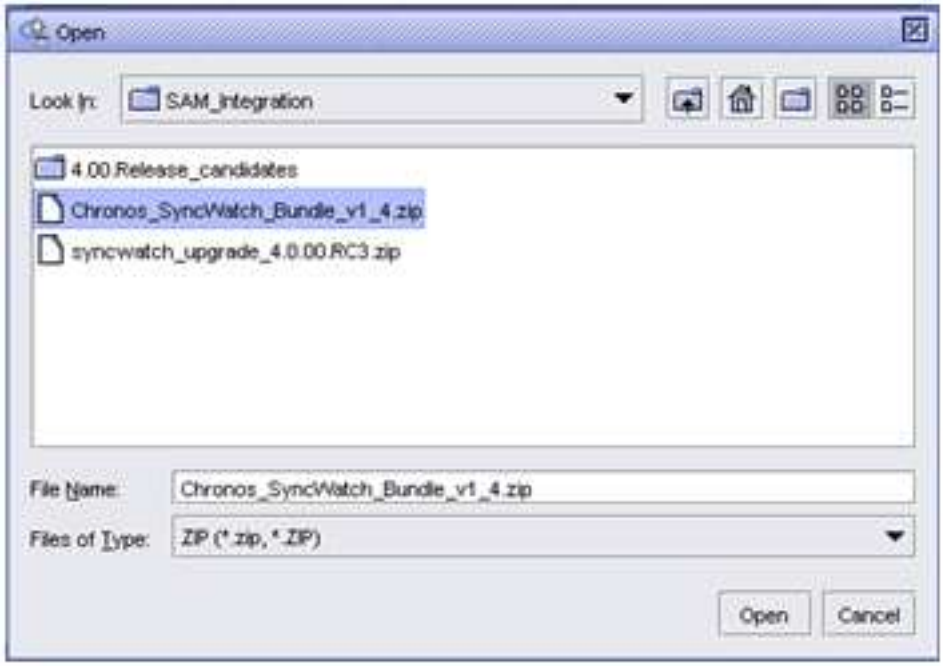
2

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

3

Navigate to the Chronos SyncWatch Bundle; see Figure 5-8, “SyncWatch script bundle” (p. 44)
.

Figure 5-8 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 5-9, “Scripts manager” (p. 45) .

Figure 5-9 Scripts manager

END OF STEPS

5.15 To execute the SyncWatch script bundle

5.15.1 Steps

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.

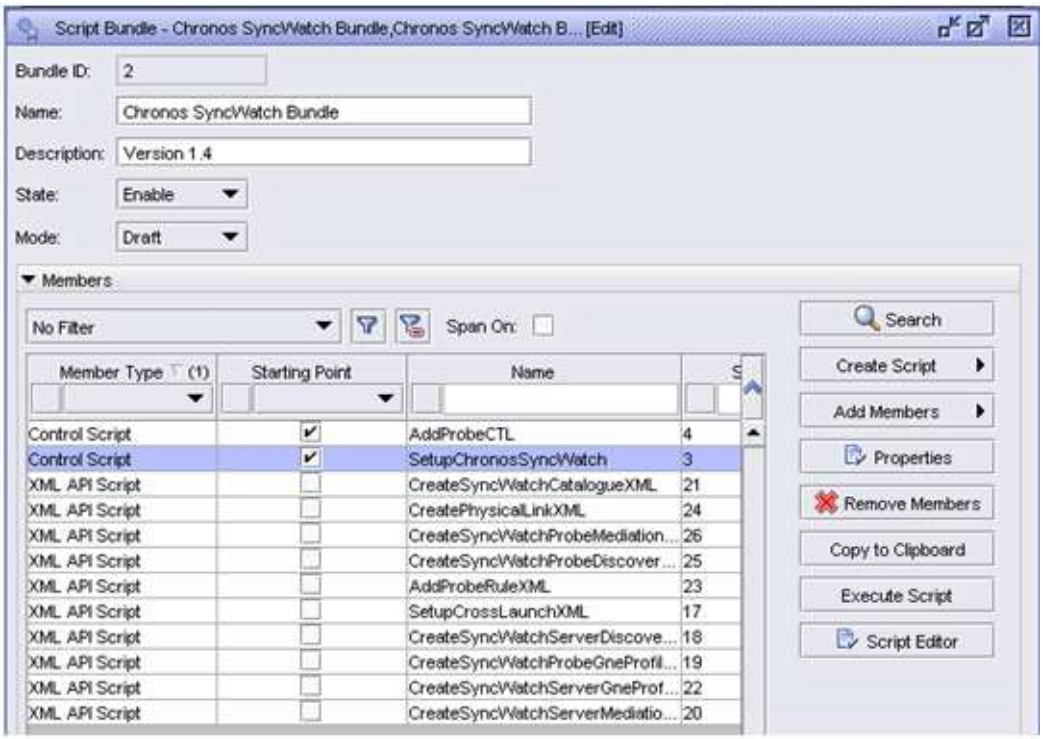
3

Select the script bundle and click on the Properties button. The Script Bundle (Edit) form opens; see Figure 5-10, “Chronos SyncWatch script bundle” (p. 46) .

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 5-10 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

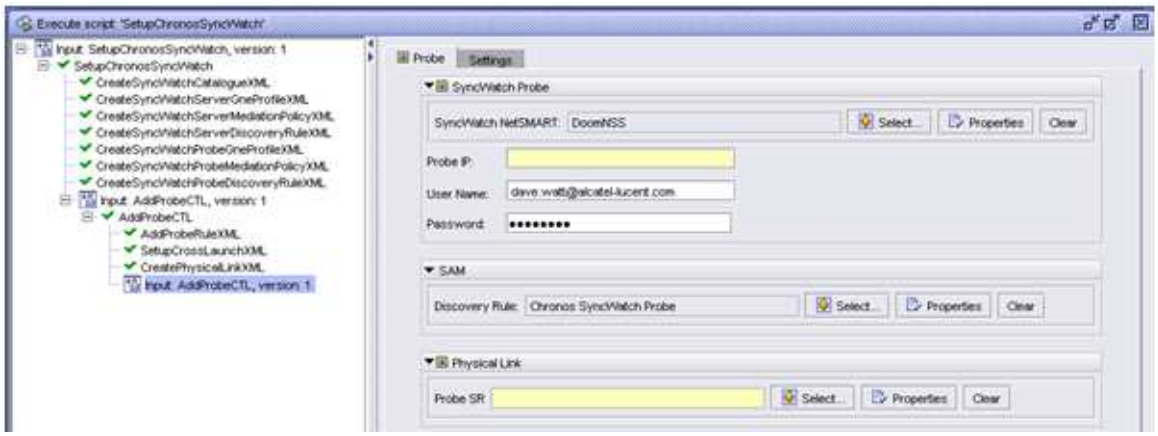
6

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.

Figure 5-11 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 Step 8 to Step 10 to configure parameters for additional SyncWatch Probes, as required.

END OF STEPS