NOKIA

NSP
Network Services Platform

Network Functions Manager - Packet (NFM-P)

Release 19.11

Integration Guide

3HE-15110-AAAD-TQZZA

Issue 1

November 2019

Legal notice

Contents

About this document

Purpose

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

Scope

NSP inter-module integration is not described in this document. For more information about such deployments, see the *NSP Deployment Overview*.

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:

- Documentation Center
- Technical support

How to comment

Documentation feedback

1 NFM-P integration with Single Sign On

1.1 Overview

1.1.1 NFM-P integration with SANE client for SSO

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.

You can gain access to the following through the SANE portal:

- NSP Launchpad
- NFM-P client GUI

After you configure the NFM-P for SANE portal access, you must configure a URL on the SANE server for each type of access that you require.

1.2 “To configure NFM-P and SANE portal integration” (p. 5) describes the NFM-P and SANE server configuration steps.

Note: A SANE client that opens the NSP Launchpad using Internet Explorer must deselect the “Do not save encrypted pages to disk” security option in Internet Explorer.

Configuring TLS

TLS is mandatory and enabled by default between NFM-P components. The TLS certificate that you intend to use for SANE access must be imported to the truststore on each NFM-P main server, as described in 1.2 “To configure NFM-P and SANE portal integration” (p. 5).

See the “TLS configuration and management” chapter of the *NSP NFM-P Installation and Upgrade Guide* for information about the NFM-P implementation of TLS.

1.2 To configure NFM-P and SANE portal integration

1.2.1 Purpose

Perform this procedure to enable NFM-P system integration with the SANE portal.

CAUTION

Service Disruption

Enabling NFM-P and SANE portal integration requires a restart of each NFM-P 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

1.2.2 Before you begin

Note: You require nsp user privileges on each main server station.

Note: You can perform this procedure as part of an NFM-P 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 NFM-P system. In a redundant system, you must perform the procedure on the standby main server first.

1.2.3 Steps

1

Perform the following steps on each main server to import your TLS certificate for SANE access to the NFM-P truststore.

Note: If the certificate is signed by a CA, you must import the entire CA chain of certificates to the truststore; see the CA documentation for information about importing trusted certificates.

1. Log in to the main server station as the root user.
2. Enter the following:

   ```
   # path/keytool -import -trustcacerts -alias alias -file
   certificate_file -keystore truststore_file -storepass password ↵
   ```

   where

   path is the path to the keytool utility

alias is the alias of the certificate to import

certificate_file is the self-signed or CA certificate file

truststore_file is the truststore file that is to hold the certificate

password is the truststore password

2

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 *NSP NFM-P 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 nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↵
   ```

4. Enter the following:

   ```
   bash$ ./nmsserver.bash stop ↵
   ```

5. Enter the following:

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

   The server status is displayed; the server is fully stopped if the status is the following:

   ```
   Application Server is stopped
   ```

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

3

Enter the following:

```
bash$ sudo samconfig -m main -sane ↵
```

The following is displayed:

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

4

Enter the following:

<main> **configure sane** ↵

The prompt changes to `<main configure sane>`

5

Enter the following:

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

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

6

Enter the following:

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

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

7

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

8

Enter the following:

<main configure sane> **back** ↵

The prompt changes to <main configure>.

9

To enable the propagation of the SANE TLS certificate to the required components, you must specify the location of the truststore file that contains the SANE certificate.

Note: You must specify the truststore location, regardless of whether the location has changed.

Enter the following:

<main configure> **tls truststore-file *truststore_file* back** ↵

where *truststore_file* is the absolute path and filename of the TLS truststore file on the main server station

10

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 start the NFM-P main server:

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

   The NFM-P main server restarts, and puts the SANE SSO configuration into effect.

5. 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.

11

To enable NSP Launchpad access, configure the following URL on the SANE server:

Note: A SANE client that opens the NSP Launchpad using Internet Explorer must deselect the “Do not save encrypted pages to disk” security option in Internet Explorer.

- https://*NFM-P_address*/cas/login?service=https://*NFM-P_address*/cas/login&client_name=SANEClient&SAMLart=%%SAML_ART%%

where *NFM-P_address* is the NFM-P main server IP address or hostname, depending on which is configured for client access

Note: Cross-launch from the SANE portal to the NSP Launchpad fails occasionally if using IE 11. If this issue is encountered, repeat the cross-launch operation from SANE.

12

To enable direct NFM-P client GUI access, configure the following URL on the SANE server:

- https://*NFM-P_address*/session-manager/login?service=https://*NFM-P_address*/?launchNFMPClient=true&client_name=SANEClient&SAMLart=%%SAML_ART%%

where *NFM-P_address* is the NFM-P main server IP address or hostname, depending on which is configured for client access

END OF STEPS

2 NFM-P integration with Chronos SyncWatch

2.1 Overview

2.1.1 Purpose

The NFM-P 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 NFM-P to configure primary or secondary PTP clocks on network elements that support timing references. See the *NSP NFM-P User Guide* for more information about configuring IEEE 1588 PTP clocks.

You can use the CPAM to manage synchronization domains and assign IP path monitors to PTP peers. See the “Synchronization management” chapter in the *NSP NFM-P 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 NFM-P provides integration support for both the SyncWatch Probe and the NetSMART Server components. The NFM-P 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.

2.1.2 Contents

2.2 Synchronization overview

2.2.1 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.

2.2.2 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.

2.2.3 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.

2.2.4 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.

2.2.5 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.

2.2.6 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.

2.3 NFM-P and Chronos SyncWatch

2.3.1 Integration overview

The NFM-P 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 NFM-P alarms
- status polling

The NFM-P 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.

2.3.2 Alarm support

By default, the NFM-P supports a limited number of standard system and interface SNMP traps for GNEs. The NFM-P 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 NFM-P also supports GNE alarm catalogs to import SyncWatch Probe traps from the NetSMART Server and translate them into NFM-P 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 NFM-P 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 NFM-P receives a GNE trap that is not one of the supported standard traps or a mapped trap in an alarm catalog, the NFM-P drops the trap. When the NFM-P 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 NFM-P.

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

Note: By default, only the NFM-P 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 NFM-P 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.

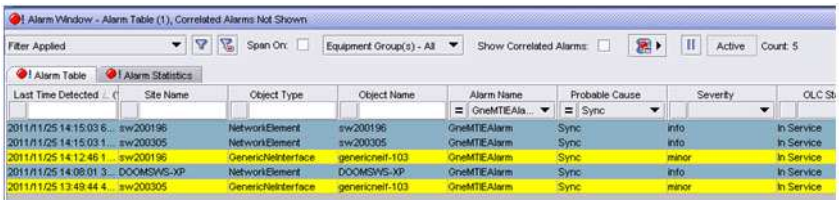
The following figure shows a SyncWatch alarm displayed by the NFM-P.

Figure 2-1 SyncWatch alarm in the NFM-P

You can view and monitor SyncWatch Probe alarms from several places on the NFM-P GUI.

- The topology map displays outstanding alarms in the top right corner of network icons. See Figure 2-4, “Topology map with physical link” (p. 27) .
- 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 2-2, “Alarm Window” (p. 15) .

Figure 2-2 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.

2.3.3 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 NFM-P release compatibility.

2.4 NetSMART Server and SyncWatch Probe in the NFM-P

2.4.1 General Information

This section describes how the NetSMART Server and SyncWatch Probe are managed in the NFM-P.

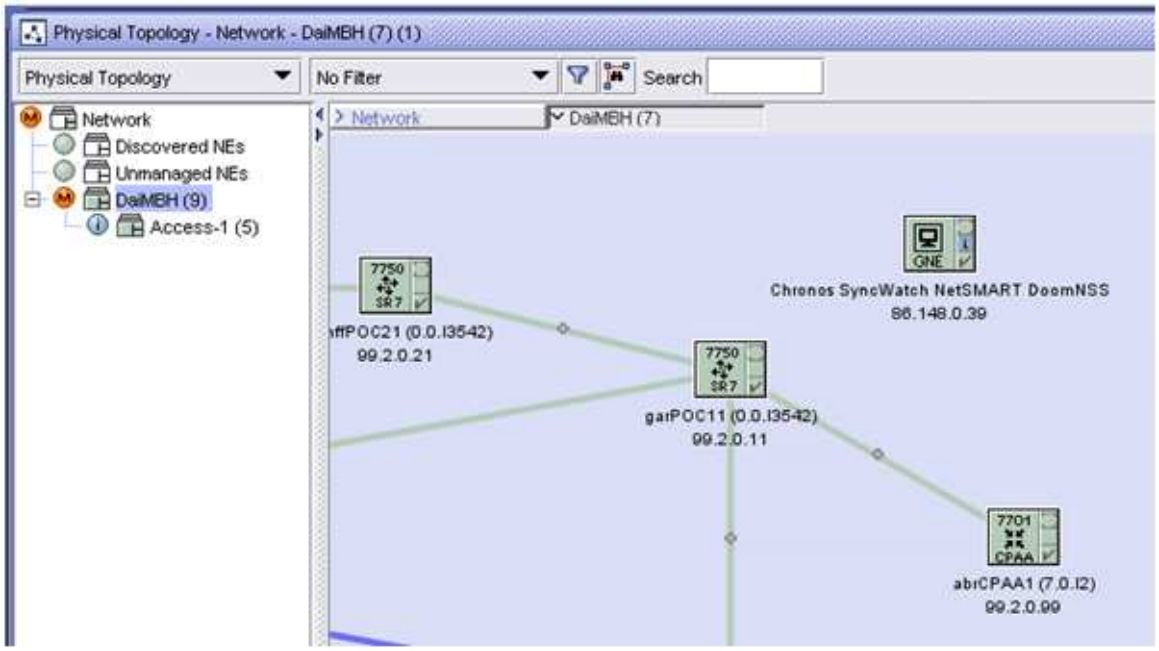
2.4.2 NetSMART Server

The NFM-P 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 NFM-P scans through the GNE profiles until it finds one that matches.

The NetSMART Server responds and the NFM-P 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 2-3 NetSMART Server on the NFM-P topology map



2.4.3 SyncWatch Probe

The NFM-P 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 NFM-P 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 NFM-P, 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 NFM-P 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 NFM-P.

2.5 Workflow for scripted SyncWatch integration

2.5.1 General Information

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

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.

2.5.2 Process

Verify SNMP communication

1

Verify from a CLI session that the NFM-P can communicate with the NetSMART Server via SNMP. See 2.8 “Verify NFM-P SNMP communication with NetSMART Server” (p. 23) .

2

Verify from a CLI session that the NFM-P can communicate with the SyncWatch Probes via SNMP. See 2.9 “Verify NFM-P SNMP communication with SyncWatch Probes” (p. 24) .

Import and execute the Chronos SyncWatch script bundle

3

Import the script bundle into the NFM-P. See 2.13 “To import the SyncWatch script bundle” (p. 28) .

4

Execute the script bundle. The NFM-P prompts you for the server IP and user information. See 2.14 “To execute the SyncWatch script bundle” (p. 29) .

Perform additional setup tasks

5

Perform a NetSMART Server cross-launch, as required. See 2.10 “To perform a NetSMART Server cross-launch” (p. 25) .

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 .

2.6 Workflow for manual SyncWatch integration

2.6.1 Overview

The following workflow describes the high-level steps that are required to manually configure SyncWatch integration with the NFM-P. 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.

2.6.2 Process

Verify SNMP communications

1

Verify from a CLI session that the NFM-P can communicate with the NetSMART Server. See 2.8 “Verify NFM-P SNMP communication with NetSMART Server” (p. 23) .

2

Verify from a CLI session that the NFM-P can communicate with the SyncWatch Probes. See 2.9 “Verify NFM-P SNMP communication with SyncWatch Probes” (p. 24) .

Note: 2.7 “Manual SyncWatch Probe integration” (p. 20) 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. The URL must have the format defined in 2.10.1 “NetSMART Server cross-launch mechanism” (p. 25) .

11

Perform a NetSMART Server cross-launch, as required. See 2.10 “To perform a NetSMART Server cross-launch” (p. 25) .

12

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

2.7 Manual SyncWatch Probe integration

2.7.1 Overview

2.5 “Workflow for scripted SyncWatch integration” (p. 18) 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 *NSP NFM-P User Guide* for more generalized descriptions and procedures about GNE integration. The sample described in Table 2-1, “SyncWatch Probe integration” (p. 21) 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 NFM-P GUI.

Table 2-1 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 an NFM-P alarm for the appropriate SyncWatch Probe. - The Interface Index Varbind Position parameter allows the trap from the NetSMART Server to generate an NFM-P 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 2.8 “Verify NFM-P SNMP communication with NetSMART Server” (p. 23) 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 NFM-P 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	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.

Table 2-1 SyncWatch Probe integration (continued)

Task	Description
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 2.9 “Verify NFM-P SNMP communication with SyncWatch Probes” (p. 24) for the Sys Object ID parameter. • Enter the SyncWatch Probe element management URL for the Default Element Manager URL parameter. - See 2.10.1 “NetSMART Server cross-launch mechanism” (p. 25) 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	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.

Table 2-1 SyncWatch Probe integration (continued)

Task	Description
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 2.10.1 “NetSMART Server cross-launch mechanism” (p. 25) for information about configuring the URL NetSMART Server cross-launch URL.
9. Create physical links between the SyncWatch Probes and a managed NE	See 2.11 “To configure a physical link” (p. 26) for information about configuring a physical link.

2.8 Verify NFM-P SNMP communication with NetSMART Server

2.8.1 Purpose

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

2.8.2 Steps

1

Open a console window.

2

Navigate to the SNMP configuration in the server binary directory:

```
bash# cd /opt/nsp/nfmp/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 NFM-P 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

2.9 Verify NFM-P SNMP communication with SyncWatch Probes

2.9.1 Purpose

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

2.9.2 Steps

1

Open a console window.

2

Navigate to the SNMP configuration in the server binary directory:

```
bash# cd /opt/nsp/nfmp/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 NFM-P 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

2.10 To perform a NetSMART Server cross-launch

2.10.1 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. 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

2.10.2 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

2.11 To configure a physical link

2.11.1 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:

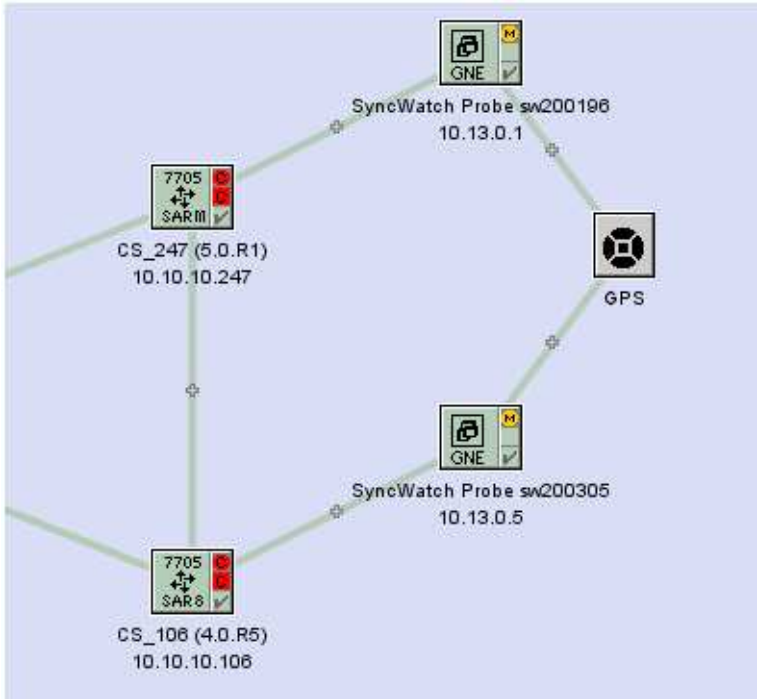
a. Configure a link representing the GPS reference input.
   1. Configure the parameters:
      - Name
      - Description
      - Endpoint A Type — choose Generic NE Interface
      - Endpoint B Type — choose Unmanaged NE
      - Notes
   2. Click on the Select button for Endpoint A to specify the GNE 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 2-4 Topology map with physical link



END OF STEPS

2.12 Chronos SyncWatch script bundle execution

2.12.1 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 *NSP NFM-P Scripts and Templates Developer Guide* for more information about script bundles and script management.

2.13 To import the SyncWatch script bundle

2.13.1 Steps

1

Choose Tools→Scripts from the NFM-P 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.

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 2-5, “Scripts manager” (p. 28) .

Figure 2-5 Scripts manager

END OF STEPS

2.14 To execute the SyncWatch script bundle

2.14.1 Steps

1

Choose Tools→Scripts from the NFM-P main menu. The Scripts manager opens.

2

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

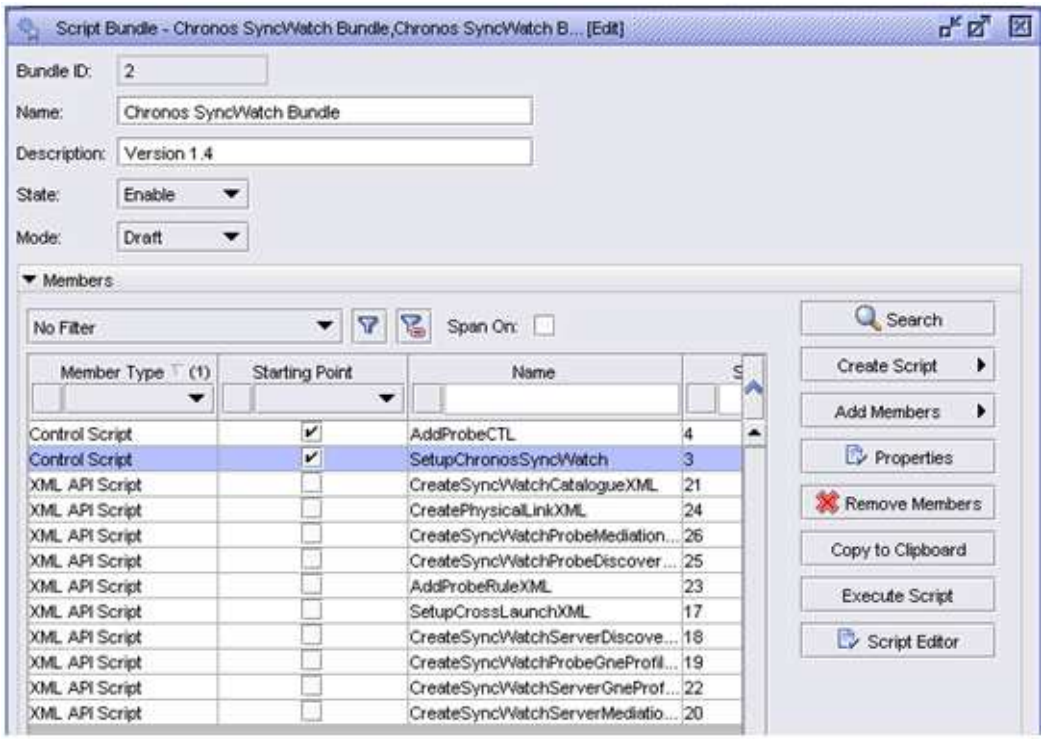
3

Select the script bundle and click on the Properties button. The Script Bundle (Edit) form opens; see Figure 2-6, “Chronos SyncWatch script bundle” (p. 28) .

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 2-6 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 NFM-P 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 NFM-P servers

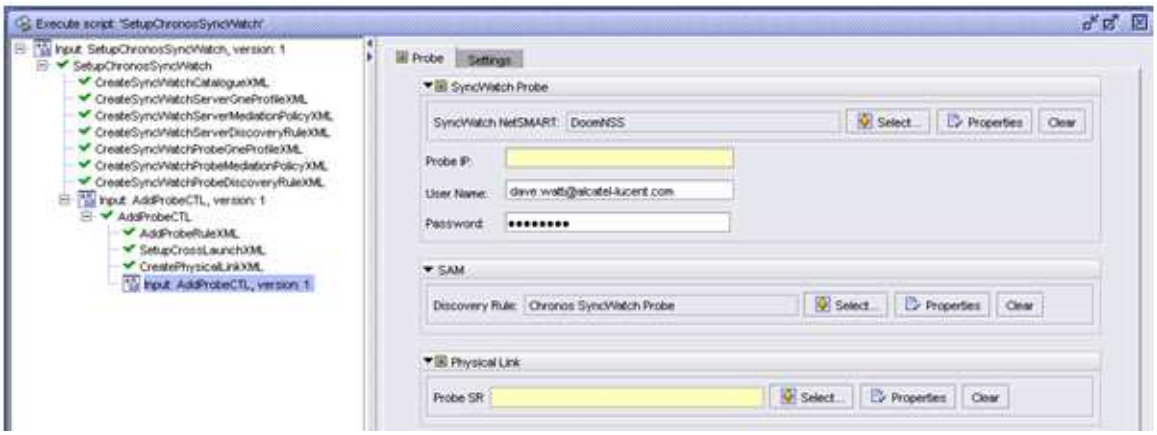
6

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 2-7 Execute script form



8

Configure the parameters:

- Probe IP — enter the IP address by which the NFM-P 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

3 NFM-P integration with other systems

3.1 Overview

3.1.1 Purpose

You can integrate the NFM-P with a variety of other systems. Integration allows the NFM-P 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

3.2 NFM-P and 5520 AMS integration

3.2.1 General Information

An NFM-P 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 NFM-P client GUI.

3.3 NFM-P and CPAM integration

3.3.1 General Information

The CPAM provides real-time control-plane IGP and BGP topology capture, inspection, visualization, and troubleshooting. The CPAM product is bundled with the NFM-P product; this integration allows the CPAM to associate routing information with NFM-P network routes, service tunnels, LSPs, edge-to-edge service traffic paths, and OAM tests. The CPAM has access to the NFM-P managed objects and displays the objects in CPAM topology views.

The 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 CPAM facilitates navigation between protocol maps and managed objects, such as protocol links.

The CPAM functions are enabled by default, and are available from the NFM-P main menu. See the *NSP NFM-P Control Plane Assurance Manager User Guide* for information about using a function.

3.4 NFM-P and DSC integration

3.4.1 General Information

The DSC is treated as a device that is managed by the NFM-P, rather than an external system that requires integration with the NFM-P. The NFM-P 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 NFM-P equipment navigation tree. The instance, Diameter proxy agent, and policy charging rule properties are viewable using the Manage→Mobile Core→DSC Instances NFM-P main menu option.

The *NSP NFM-P LTE EPC User Guide* describes DSC discovery and management using the NFM-P.

3.5 NFM-P and EM systems integration

3.5.1 General Information

The NFM-P can manage multiple element manager systems using the Horizontal Integration Protocol (HIP). The HIP allows EM systems to integrate with the NFM-P using a single jar file (the HIP library jar file). When integrated with the NFM-P, the EM system's inventory and alarm information are displayed in the NFM-P GUI. Any operations performed on the EM system's alarms using the NFM-P 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 NFM-P NEs. For more information about discovering EM systems, see the *NSP NFM-P User Guide*.

The HIP library jar file is provided with the NFM-P 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 NFM-P simulator simulates an NFM-P 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 NFM-P 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.

3.6 NFM-P and LTE OMS integration

3.6.1 General information

The LTE OMS is the managed NE that acts as the communication interface between the NFM-P and Flexi MR BTS and provides all information about RAN nodes to the NFM-P managed network. The LTE OMS and the NFM-P communicate using an NWI3 variant of CORBA. See the *NSP NFM-P MultiRadio BTS User Guide* for more information.