NOKIA

NSP
Network Services Platform
Network Functions Manager - Packet (NFM-P)
Release 23.11

Control Plane Assurance Manager User Guide

3HE-19005-AAAC-TQZZA
Issue 1
December 2023

Legal notice

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Contents

About this document

Purpose

The *NSP NFM-P Control Plane Assurance Manager User Guide* provides information about using the CPAM feature set and CPAA route analyzer to capture real-time control IGP topology information for inspection, visualization, and troubleshooting.

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

Please send your feedback to documentation.feedback@nokia.com.

Part I: Getting started

Overview

Purpose

This volume provides an introduction to the CPAM.

Contents

1 CPAM overview

1.1 Introduction to the NFM-P Control Plane Assurance Manager

1.1.1 General information

The CPAM feature set provides real-time control-plane IGP and BGP topology capture, inspection, visualization, and troubleshooting functions. The CPAM is fully integrated with the NFM-P; the integration enables 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 provides assurance against routing malfunctions, rapid problem resolution, and cost-effective scaling of the service provider IP/MPLS Network Operations Center (NOC) via simpler tools for new hires or staff redeployment.

The CPAM functions are available from the NFM-P main menu, and support network management activities such as the following:

- **Planning**

  Planning activities are optimized using real-time topology updates and strong linkages between services and infrastructure layers.

- **Management**

  Real-time topology updates and multi-layer highlighting allow the rapid assessment of service, tunnel, and routing states on the IGP and IP/MPLS maps.

- **Troubleshooting**

  Historical OAM trace, SPF and RSVP path monitoring, and checkpoints allow you to rapidly detect and resolve service-level issues for which the root cause is in the control plane.

  Troubleshooting functions include:

  - Path Computation—query the routing plane for its current forwarding decision between endpoints for IGP (SPF/CSPF), BGP prefixes (exit router) or multicast tree (source, group)
  - IP/LSP/SDP/Service Highlight—highlight the possible forwarding paths LSPs (primary, standby, secondaries), SDP (GRE, LDP, CoS, Backup, Load Balancing, Discarding), services (VLL, VPLS, VPRN, IES)
  - IGP/BGP/MP-BGP/Path History—history derived from routing update analysis, checkpoints and statistics. Graphical IGP analysis (map roll-back), checkpoint comparisons, 7-day prefix stability computation.
  - Impact Analysis—categorized changes to the SDP/service and composite services using a given IGP link, an LSP, or an IP path over a period of time.

- **Restoration**

  Checkpoints and real-time views of IP/MPLS, service, and service tunnel infrastructure allow you to restore network topologies.

- **Assurance**

Alarms, network route and tunnel inspection lists, validation functions, checkpoints, and multi-layer views reveal routing faults as they occur.

Assurance functions include:

- Network Audit—facilitates the detection of configuration error graphically, via highlights or automated audits of the network.
- Protocol, Network and Path Monitoring—detection of abnormal routing activity in the network and alarm notification. Routing flaps, prefix unreachability, path delay/jitter exceeded after reroute, diverging paths, routing table drop or jump for Internet and VPRN, etc.
- Network Simulation—offers the ability to change the routing configuration of the current network or add/remove new routers/links to verify its impact on paths before committing the changes in the real network. This capability is intended for the NOC to verify the impact of upgrade nodes or of failing a link, etc.

1.1.2 CPAM scope of command roles

Permissions for CPAM functions are controlled by the scope of command profiles assigned to user groups. A scope of command profile contains a set of scope of command roles; see the chapter on NFM-P user security in the *NSP System Administrator Guide* for more information.

To perform functions in the CPAM feature set, user groups must be assigned a scope of command profile with the required scope of command roles.

A system administrator can configure custom scope of command roles to assign permissions. The NFM-P also provides predefined scope of command roles.

The following predefined scope of command roles are specific to CPAM functions:

- CPAM Management
- CPAM OSS PCA
- CPAM Topology Simulator
- Root Cause Analysis (RCA) Object Verification

See the *NSP System Administrator Guide* for descriptions of predefined scope of command roles and assignable permissions.

1.1.3 CPAM functions

The two main components to the control plane assurance management solution are:

- the CPAM feature set
- a CPAA route analyzer

The CPAM feature set includes control frameworks, applications, and co-ordination functions for the distributed CPAAs. The CPAM also processes the CPAA data.

The CPAM Java processing engine communicates with GUI and XML API clients using the NFM-P API.

The CPAM retrieves data directly from a CPAA. It aggregates and analyzes data from multiple CPAAs and data collected by the NFM-P. In addition, the CPAM co-ordinates CPAA activities for

functions that require the participation of more than one CPAA, for example, an IP-to-IP SPF route calculation that involves multiple areas.

Each IGP administrative domain must be connected to at least one CPAA. The CPAM can communicate with the CPAAs through the following channels:

- proprietary protocol over TCP
- SNMPv2c or SNMPv3
- CLI over Telnet or SSH2

Most of the communication that occurs between the CPAM and CPAAs, such as routing updates, TCA, and SPF requests and responses, is over TCP. SNMP is used for CPAA configuration management. A CLI is required for system commands required for device commissioning.

The CPAM discovers CPAAs over the SNMP channel. Each CPAA gathers LSDB information from network areas and reports the information and subsequent routing events or alarms to the CPAM over the TCP channel.

1.1.4 CPAA route analyzer

The CPAA uses a passive version of the 7750 SR OS, and acts as a special-purpose routing element that passively peers with the network to capture a real-time view. The NFM-P manages a CPAA as a network device.

The CPAA collects and analyzes routing data from the routing areas to which it is connected. Traffic on the CPAA is restricted to control data and packages directly destined to the CPAA. Because no other traffic can pass through it, the CPAA only advertises itself to its neighbor routers and does not re-advertise link-state data received from its neighbors.

The following are the main functions of a CPAA:

- listening to routing data from the routing protocols that are running on it
- providing route calculation for routes passing through the routing areas the CPAA is responsible for
- performing routing analysis and providing the results to the CPAM, so the CPAM can generate network-wide reports or alarms

1.2 CPAA under NFM-P management

1.2.1 General information

The 7701 CPAA and vCPAA are managed by the NFM-P like any other NE. Management procedures such as timing synchronization, polling, deployments, and NE resynchronization, are similar to procedures for other SR OS devices. See the *NSP NFM-P Classic Management User Guide* for information about general device management functions. The scope of commands on the CPAA is much smaller than those of any other SR-based router.

The CPAA can be managed in-band or out-of-band under the NFM-P. Out-of-band management is performed through the management port of the CPAA. For in-band management, the network must

be able to route traffic to the CPAA using the system IP address of the CPAA. In-band management is possible only if the port on the router that is physically connected to the CPAA is in network mode.

1.2.2 Operating system configuration

The CPAA OS is based on the 7750 SR OS. The CLI configurations and management for the CPAA are a subset of the 7750 SR.

1.2.3 CPAA alarm support

All alarms supported in CPAA Release 8.0 are also supported in CPAA Release 9.0 and CPAA Release 10.0.

The 7701 CPAA hardware rev.2 and vCPAA do not support power supply alarms or power failure alarms. The CPAA OS has no visibility of the power supply, and cannot detect power interruptions.

1.2.4 Out-of-band management

The CPAM and CPAA use two TCP channels: an SNMP/UDP channel for event notifications, and a CLI over Telnet/SSH2 session for general communication.

The TCP channels can be configured as out-of-band so that the events and control data are carried over a separate management network. In such a case, the CPAA management address is different from the system IP address.

1.2.5 IGP administrative domains

An IGP administrative domain is a routed network that contains, for each OSPF and IS-IS, one backbone. An IGP administrative domain can have both an OSPF and IS-IS backbone at the same time. For OSPF, it is assumed that there cannot be multiple instances of any area within an admin domain. An IGP administrative domain is uniquely identified by a domain number and name. A CPAA which is configured with an IGP role is assigned to each IGP administrative domain.

1.2.6 BGP AS administrative domains

An administrative domain which represents the standard BGP AS, confederation AS, or sub-AS. A BGP confederation AS administrative domain contains other BGP sub-ASs. A BGP AS is identified by a BGP AS number, which should be identical to the network-configured BGP AS, a BGP AS name, and BGP AS type. Each BGP AS administrative domain is associated with only one IGP administrative domain. An IGP administrative domain can be associated with several BGP AS administrative domains. A CPAA which is configured with a BGP role must be assigned to each BGP AS administrative domain. Each CPAA can be assigned to only one BGP AS administrative domain.

1.2.7 Routing protocols

When interacting with OSPF routing protocols, the CPAA establishes normal OSPF neighborships, but prevents other routers from routing through it by advertising its own OSPF links with a metric of 65535. The CPAA only advertises its own links, so in addition to the metric, traffic cannot be routed through the CPAA. The CPAA system address and its interfaces will appear in the OSPF routing table of the other nodes in the network.

When interacting with BGP routing protocols, the CPAA estabilishes normal BGP peerings, but does not advertise any BGP prefixes.

1.2.8 Routing domains

A CPAA is connected to the IGP routing plane in the same way an IGP router—OSPF or IS-IS—is connected to its neighbors.

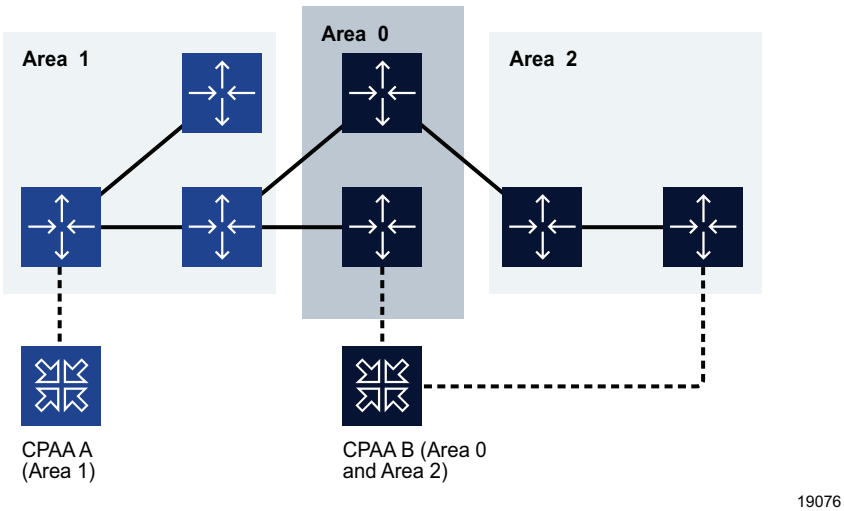
A CPAA can be connected to several OSPF routing areas, and to both IS-IS L2 and L1 routing domains. In addition, a CPAA can have multiple interfaces to a routing domain. There can be only one active interface for any routing domain. A CPAA can be connected to an OSPF and an IS-IS network at the same time.

Note: All of the CPAAs must be connected to routing domains in the same IGP administrative domain.

The CPAM supports OSPFv2.

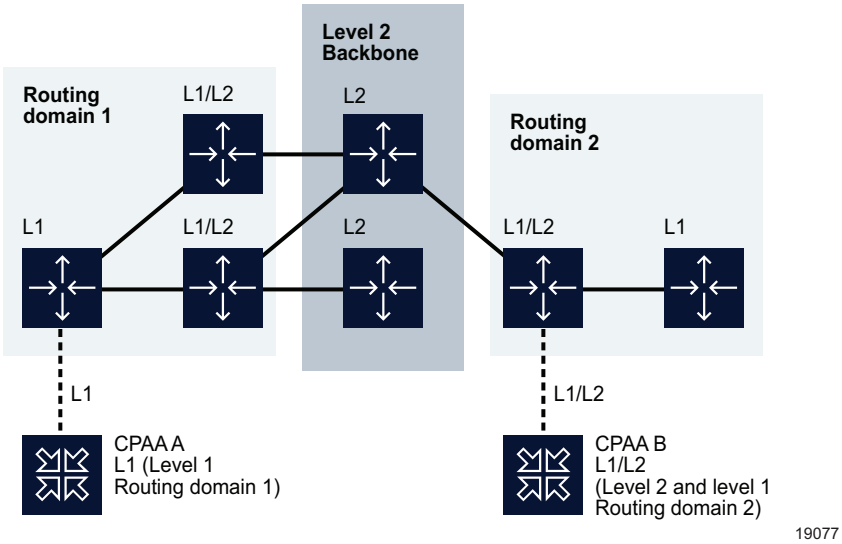
The following figure shows an OSPF network with three areas: 0 (backbone), 1, and 2. CPAA A is responsible for Area 1. CPAA B is responsible for Areas 0 and 2.

Figure 1-1 CPAAs connected to an OSPF network



The following figure shows an IS-IS network with two level-1 routing domains and a level-2 backbone. CPAA A is responsible for level-1 Routing domain 1 over the L1 link. CPAA B is responsible for the level-2 backbone and the level-1 Routing domain 2 over the L1/L2 link. L2 routers must not explicitly belong to an routing domain.

Figure 1-2 CPAAs connected to an IS-IS network



1.2.9 CPAA network connections

The number of CPAAs deployed in the network is determined by the number of IGP areas, the router count per area, the backhaul strategy, the protocols deployed, the amount of monitoring required, and the BGP architecture (confederation, mesh or route reflector). Scalability limits can be found in the *NSP Planning Guide*. To determine the number of CPAAs required for a particular deployment, contact your Nokia representative.

For OSPF, the CPAA allows the configuration of multiple interfaces for an OSPF area. Of these interfaces, there can be multiple physical IGP interfaces— interfaces that are bound to a port— but only one logical interface, such as the system interface. No other loopback interface is allowed. The NFM-P also enforces this restriction for 7750 SR routing configuration. To prevent data traffic from passing through it, the CPAA does not send type 3, 4, or 5 LSP information to its neighbors. No LSP information is sent from one area to another.

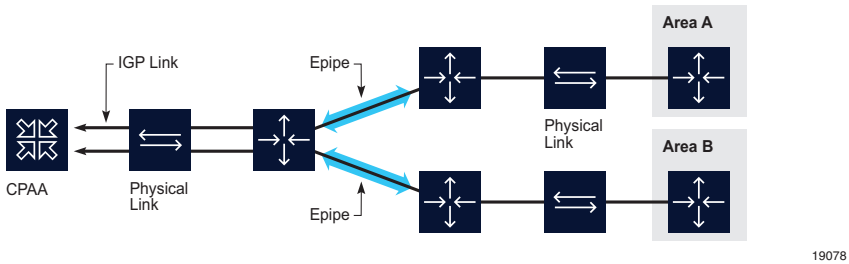
For IS-IS, there is only one active L1 link and one active L2 link from a CPAA. This restriction guarantees that there is only one link to each L1 IS-IS routing domain, which could use multiple area IDs. More than one L1 link can be configured, but all of the links must use the same area ID. All L1 links can be in an Adjacency Up state, which is equivalent to FULL state in OSPF, but the CPAA sends the LSP of the active link only.

Note: Because only one active IGP link to a routing area or level can exist and the CPAA does not act as an ABR router, traffic that is not destined to it should never be sent to the CPAA. This data can still reach the CPAA in some cases.

To ensure that all of the traffic that is not destined to the route listener is dropped, it is strongly recommended that you create a routing policy for all of the routers connected to the CPAA.

Multiple IGP interfaces can share the physical interface where each protocol interface occupies a VLAN ID. If the neighbors of the CPAA are not physically attached to the CPAA, IGP links can be carried over VLL Epipes. The following figure shows two remote areas (A and B) that are connected to the CPAA over VLL Epipes.

Figure 1-3 CPAAs connected to routing areas through VLL Epipes



1.2.10 CPAA link redundancy

A CPAA can have multiple IGP interfaces to one routing area. The CPAA advertises the LSA/LSP for only the active link of the redundant pair.

For example, a router and a CPAA are connected through two interfaces, both in the same OSPF or IS-IS area. Three unidirectional links—two links from the router and one link from the CPAA—appear on the topology map because the CPAA advertises only the active link. The standby link from the CPAA is not displayed on the topology map. The following sequence of events occurs:

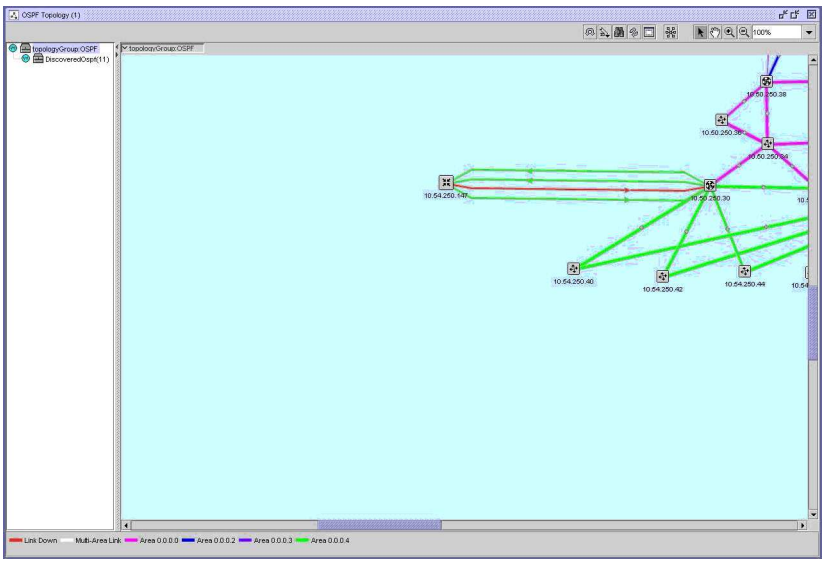
- the user applies a checkpoint to the topology
- a fault occurs and the active link A becomes operationally down
- the standby link B becomes operationally up and becomes the active link B that is advertised by the CPAA

The CPAA informs the CPAM that the active link A (now a standby link) is deleted and a new active link B has been added. The following links appear on the topology map, as displayed in Figure 1-4, “CPAA redundancy example” (p. 24) :

- from the CPAA
  - one red operationally down link (active link A in checkpoint-applied topology)
  - one green operationally up link (active link B added after the checkpoint was applied)
- from the router
  - two green operationally up links (router links in checkpoint-applied topology)

See Chapter 18, “Impact analysis” for information about link colors and topology checkpoints.

Figure 1-4 CPAA redundancy example



Part II: Commissioning and system administration

Overview

Purpose

This volume describes commissioning and maintenance activities to be performed on the CPAM.

Contents

2 CPAM commissioning configurations

2.1 Workflow to commission the CPAM

2.1.1 Purpose

This workflow outlines the high-level steps necessary to commission the CPAM.

2.1.2 Stages

1

Create IGP administrative domains. See 10.4 “To configure an IGP administrative domain” (p. 196) for more information.

2

Create BGP ASs. See 10.5 “To create a BGP standard AS” (p. 196) or 10.6 “To create a BGP confederation AS” (p. 197) for more information.

3

Create group routers on the topology map. See 4.10 “To create user-defined groups on topology maps” (p. 62) for more information.

4

Manage topology references in the IGP administrative domain. See 6.3 “To manage topology references in an IGP administrative domain” (p. 82) for more information.

5

Create, configure, view and compare checkpoints. See 18.14 “To create an OSPF checkpoint” (p. 367) to 18.21 “To create an Admin Domain checkpoint schedule policy” (p. 373) .

6

Configure alarm thresholds. See 16.3 “To configure alarm thresholds” (p. 295) for more information.

7

Configure and turn on IP and LSP monitoring. See 8.3 “To monitor an IP network path” (p. 135) and 8.5 “To monitor a dynamic LSP” (p. 139) for more information.

8

Configure BGP prefix monitoring. See 8.15 “To configure BGP monitored prefixes” (p. 157) for more information.

9

Configure BGP RIB. See 10.12 “To view BGP RIB information” (p. 204) for more information.

10

Configure VPN capture. See 10.9 “To retrieve BGP information from a CPAA” (p. 201) for more information.

11

Configure the size constraint for path record history retention. See 8.16 “To configure the size constraint limit for path monitor records” (p. 158) for more information.

12

Configure topology map information tables. See 7.34 “To use the Configure Info Tables button” (p. 124) for more information.

3 CPAM routine system maintenance

3.1 Overview

3.1.1 Purpose

This section is intended for NFM-P operators that are responsible for developing and using maintenance procedures in CPAM implementations.

The CPAM maintenance tasks and procedures are categorized by frequency. Nokia recommends the implementation of a regular maintenance schedule to help you to be proactive about the state of the control plane.

3.1.2 Managing CPAM alarms

In large NFM-P-managed networks where applications are constantly interacting with a busy network in a non-stop management environment, many alarms are raised. These alarms should be:

- tracked as they arrive
- historically logged for trend and performance analysis

You must review CPAM alarms on a daily basis to check the type and characteristics of the alarms, and to resolve the problems associated with the alarms. You can create search filters to identify alarms, and view up to six filtered alarm lists to monitor network-wide issues. You can analyze the alarm history log to identify chronic or prolonged failures, or trends.

3.2 CPAM daily system maintenance workflow

3.2.1 Purpose

This workflow outlines the high-level steps necessary to maintain the CPAM feature set on a daily basis.

3.2.2 Stages

1

Open OSPF, ISIS, MPLS, and PIM topology maps from the NFM-P main menu and check for newly discovered routers. See 4.7 “To open a topology map from the NFM-P main menu” (p. 61) for more information.

2

Manually retrieve BGP AS path, RIB Info and IP VPN route targets. See 10.9 “To retrieve BGP information from a CPAA” (p. 201) for more information.

3

Manually retrieve PIM domain PIM and IGMP state information. See Chapter 17, “Multicast

manager" for more information.

4

Check for newly created OSPF, ISIS, BGP, and Path Monitor alarms. See 3.5 "To list all incoming alarms" (p. 31) , 3.6 "To store alarms in an alarm history log and view alarm history logs" (p. 32) , and 3.7 "To create search filters for CPAM alarms" (p. 33) for more information.

5

Schedule database backups. See the *NSP System Administrator Guide*.

3.3 CPAM weekly system maintenance workflow

3.3.1 Purpose

This workflow outlines the high-level steps necessary to maintain the CPAM feature set on a weekly basis.

3.3.2 Stages

1

Check for the following Path Monitor historical records:

- IP Path Monitor records with a status != "noError" (no route found)
- IP Path Monitor records with Auto OAM Result Status != "Succeeded" (path found, ping and trace may have failed)
- LSP Path Monitor records with a status != "noError" (no route found)
- LSP Path Monitor records with Auto OAM Result Status != "Succeeded" (path found, ping and trace may have failed)

See 8.17 "To view IP path records" (p. 159) and 8.18 "To view LSP path records" (p. 160) for more information.

2

Verify the status of the primary and standby database. See the *NSP System Administrator Guide*.

3

Verify the status of the primary and standby NFM-P main servers. See the *NSP System Administrator Guide*.

3.4 CPAM monthly system maintenance workflow

3.4.1 Purpose

This workflow outlines the high-level steps necessary to maintain the CPAM feature set on a monthly basis.

3.4.2 Stages

1

As required, delete OSPF and ISIS checkpoints.

2

Clean up OSPF and ISIS references in each IGP administrative domain. See 6.3 “To manage topology references in an IGP administrative domain” (p. 82) for more information.

3

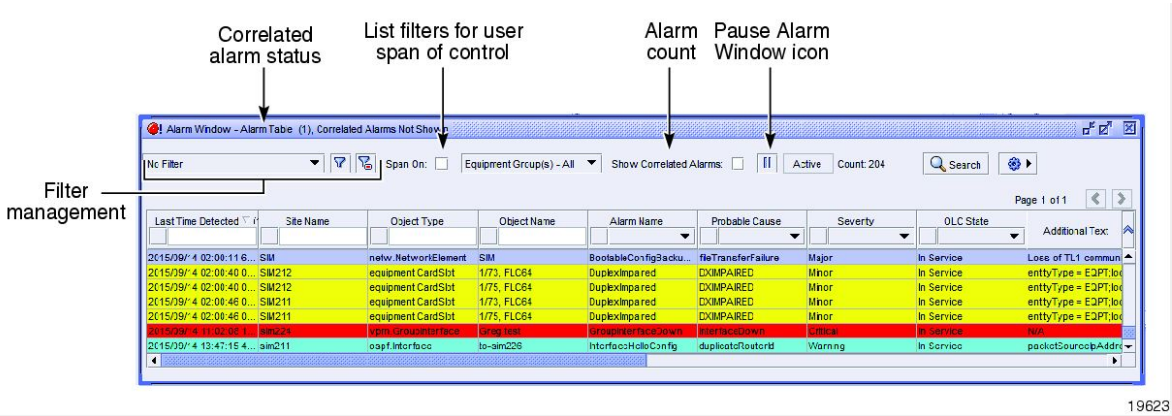
Back up CPAA configuration files. See 3.8 “To create a CPAA backup policy” (p. 35) for more information.

3.5 To list all incoming alarms

3.5.1 General information

The dynamic alarm list allows you to monitor all incoming alarms, as displayed in the following figure:

Figure 3-1 Dynamic alarm list



3.5.2 Steps

1

Ensure that the Alarm Table tab in the Alarm Window at the bottom of the NFM-P client GUI is selected.

2

Right-click on an alarm entry row.The contextual alarm menu appears.

3

Handle the alarms according to your company alarm policies.

For example, to acknowledge an alarm and then delete the alarm:

1. Choose Acknowledge Alarm(s) from the contextual menu.

   The Alarm Acknowledgement form appears.
2. Modify the Severity and Urgency parameters, as required.
3. In the Acknowledgement Text parameter, enter data about the alarm, according to your company alarm policies.
4. Click on the OK button.
5. Confirm the action.

   The Ack column in the alarm row indicates that the alarm is acknowledged.
6. Right-click on the alarm entry row.

   The contextual alarm menu appears.
7. Choose Delete Alarm(s) from the contextual menu to delete the alarm.

   Caution: You cannot recover a deleted alarm unless you store alarms in the alarm history log. Perform 3.6 “To store alarms in an alarm history log and view alarm history logs” (p. 31) to store the alarm in the history log.
8. Confirm the action. The alarm is deleted.

END OF STEPS

3.6 To store alarms in an alarm history log and view alarm history logs

3.6.1 Steps

1

Choose Administration→Alarm Settings from the NFM-P main menu. The Alarm Settings form appears.

2

Click on the Alarm History DB Behavior tab.

3

Set the alarm history behavior:

1. Specify the Max 24hr Partition Log Size (records) parameter to set the maximum number of entries in the alarm history log.
2. Ensure that the Administrative State parameter is set to Up to enable alarm history logging.
3. Select the Log on Change check box to specify whether to log an alarm when one of its properties changes, for example, to log an alarm when the alarm is acknowledged.

4. Select the Log on Deletion check box to specify whether to log an alarm when it is deleted.

   Note:

   Nokia recommends that you select the Log on Deletion option to ensure that there are logged records of all deleted alarms saved as historical alarm records.

4

Set filters to the DB policy to determine the criteria for an alarm to be logged:

1. Click on the Set Purge Range button. The Alarm Settings Filter form opens.
2. Configure the list filter criteria.
3. Click on the OK button.

5

Delete the alarms according to your alarm handling policies.

The deleted alarms are logged to the alarm history logs. To view logged alarm history records:

1. Choose Tools→Historical Alarms from the NFM-P main menu. The Alarm History filter form opens.
2. If required, configure the filter criteria to limit the range of historical alarms displayed.
3. Click on the Search button. The historical alarms appear based on the filtering criteria.

   Note:

   When you sort more than 50 000 outstanding or logged alarms, GUI performance is affected. Use filters to limit the number of alarms that are listed.

6

Review the alarm history log data for trends and other fault management purposes. Transfer the data from the NFM-P for post-processing, as required.

END OF STEPS

3.7 To create search filters for CPAM alarms

3.7.1 General information

You can create and select filters to view specific CPAM alarms in the dynamic alarm list. You can save multiple filters and view the alarm information by opening up to 6 alarm windows. The name of the filter appears in the alarm window title of each alarm window that is open. Viewing CPAM alarms using the dynamic alarm list is described in 3.5 “To list all incoming alarms” (p. 31) . Figure 3-1, “Dynamic alarm list” (p. 31) shows the location of the Manage Filters icon in the alarm window.

3.7.2 Steps

1

Choose Application→Alarm Window from the NFM-P main menu. The Alarm Window opens.

2

Click on the Filter icon next to the Filter drop-down menu. The Alarm Window - Alarm Table form opens.

3

Configure the list filter criteria:

1. Choose Alarm Type from the Attribute menu.
2. Choose EQUALS from the Function menu.
3. Choose one of the following from the Value menu:
   - ConfigurationAlarm
   - topologyAlarm
4. Click on the Add button.
5. Repeat 1 to 4 to add additional filters.

4

Click on the Save button. The Save Filter form opens.

5

Configure the parameters:

- Filter Name
- Description
- Public

6

Click on the Save button. The Save Filter form closes and the Alarm Window - Alarm Table form reappears.

7

Click on the OK button to close the Alarm Window Refine Form.

8

Click on the Select Filter drop-down menu. The saved search filter appears in the select filter drop-down menu list.

9

Click on the saved search filter to load and view the results of the search in the dynamic alarm list. The number of alarms associated with the selected search filter appears in the Count field, as displayed in Figure 3-1, “Dynamic alarm list” (p. 31) .

END OF STEPS

3.8 To create a CPAA backup policy

3.8.1 General information

When the NFM-P performs a CPAA configuration backup, it transfers files to itself from the CPAA.

3.8.2 Steps

1

Choose Administration→NE Maintenance→Backup/Restore from the NFM-P main menu. The Backup/Restore form opens.

2

Click on the Backup/Restore Policy tab, then click on the Create button. The Backup Policy (Create) form opens.

3

Specify whether the backup function is enabled.

a. Enable the Enable Backup parameter.

b. Disable the Enable Backup parameter. The remaining parameters on the form cannot be configured. Go to Step 10 .

4

Configure the parameters:

- Policy ID
- Auto-Assign ID
- Name

5

Ensure the Policy Type is set to SR Based Node.

6

CAUTION

Service Disruption

When you use the NFM-P client GUI to restore a CPAA configuration and you disable the Auto-Reboot After Successful Restore parameter, there is a risk that the bof.cfg file may be overwritten in the following situations:

- when a user performs “bof save” using CLI on the CPAA
- If there is a gap between a restore and a reboot, perform a “show bof” to ensure that another user has not performed a “bof save”.

Specify whether to perform a reboot after the configuration is restored to the device by specifying the Auto-Reboot After Successful Restore parameter.

7

You can schedule backups based on a time interval or on the number of CPAA configurations performed from the NFM-P server. Configure the backup triggering parameters:

- Scheduled Backup Scheme
- Scheduled Backup Interval
- Scheduled Backup Sync Time
- Scheduled Backup Threshold (operations)
- Auto Backup Scheme
- Auto Backup Threshold (operations)

8

Configure the Backup Settings parameters:

- CLI Config File Mode
- CLI Config Save Details
- CLI Debug Save Config File Mode
- Boot Option File Mode
- File Compression

Note: In addition to enabling the CLI Debug Save Config File Mode parameter, you must specify the location of the debug configuration files in the nms-server.xml file.

9

Configure the parameters in the Backup Purging panel. Backup purging parameters allow you to specify the number of backup files kept. These settings allow you to eliminate manual monitoring and deletion of backup files. The purge criteria can be the number of files, the age of the files, or both.

- Auto-Purge Scheme
- Number of Backups
- Maximum Backup Age (days)

10

Click on the OK button to save the backup policy. The Backup Policy (Create) form closes.

11

Assign the policy to CPAAs as required.

1. Select the new policy in the list and click on the Properties button. The Backup Policy (Edit) form opens.
2. Click on the Backup/Restore Policy Assignment tab.

3. Select one or more CPAAs in the Unassigned Sites list and click on the right-pointing arrow to move them to the Assigned Sites list.
4. Click on the OK button. The Backup Policy (Edit) form closes and a dialog box appears.
5. Click on the Yes button. The policy is assigned to the NEs.

12

Close the Backup/Restore form.

END OF STEPS

Part III: Topology

Overview

Purpose

This volume provides information about the CPAM topology.

Contents

4 Topology management

4.1 CPAM topology overview

4.1.1 Introduction to CPAM network topology

You can view the following network topology maps on the CPAM:

- IGP topology
- OSPF topology
- OSPFv3 topology
- ISIS topology
- MPLS topology

Note: See Chapter 5, “MPLS topology management” for information about MPLS topology maps.

Topology maps display real-time network topology information. The coordinates are synchronized for all of the routers in the network. If a router is also managed by the NFM-P, the NFM-P physical layer map (L1) coordinates may not be the same as the CPAM coordinates.

A map toolbar, which consists of a view selector and a collection of buttons, is used to manage the map views.

4.1.2 CPAM administrative domains

WARNING

Equipment Damage

The IGP administrative domain should generally be public IP address spaces, and not private IP address spaces. If two different IGP administrative domains have duplicate router IDs, for example, some functionality—such as the IP Path Monitor and Managed Routes—may not work correctly.

An administrative domain is a user-configured grouping that represents a logical routed network. The CPAM supports the following administrative domains:

- **IGP administrative domain**
  A routed network with OSPF, ISIS, or both protocols running. There can be only one backbone domain for each protocol. For OSPF, multiple areas with the same area ID cannot exist.
- **BGP AS**
  An administrative domain which represents the standard BGP AS, confederation AS, or sub-AS. A BGP confederation AS administrative domain contains other BGP sub-ASs.

An IGP administrative domain is uniquely identified by a domain number and name that are configured at creation. A CPAA which is configured with an IGP role must be assigned to an IGP administrative domain. Each CPAA can be assigned to only one IGP administrative domain. A BGP AS is identified by a BGP AS number, which should be identical to the network-configured BGP AS,

a BGP AS name, and BGP AS type. Each BGP AS administrative domain is associated with only one IGP administrative domain. An IGP administrative domain can be associated with several BGP AS administrative domains. A CPAA which is configured with a BGP role must be assigned to each BGP AS administrative domain. Each CPAA can be assigned to only one BGP AS administrative domain.

See Chapter 10, “BGP management” for information about BGP network management.

4.1.3 Flat maps

A flat map is available for the CPAM by choosing Tools→Route Analysis→Flat Maps from the main menu. The map options available using a flat map are:

- IGP Topology
- OSPF Topology
- OSPFv3 Topology
- ISIS Topology
- MPLS Topology
- Multicast Topology

The flat map is used to view a large number of network objects and links. Double-click on a object in the flat map to display the properties of the object.

The flat map provides similar navigation and functionality to other topology maps, such as:

- object icons in the flat map are displayed at a reduced size, link lines are thinner, and object details are not displayed
- mouse-based navigation
- zoom in and out
- NE and link status color
- link group expand/collapse

The flat map supports up to 1000 objects and 8 links per object. To narrow the range of objects that are displayed in a flat map, you can create, name, and save multiple filters by creating filter definition trees.

You can also click on the Display Filterable Flat Map button to quickly display a flat map of the current topology map view.

Filter definition tree

A filter definition tree allows you to apply one or more filters to a map view to narrow the range of objects that are displayed. Filter definition trees can be saved for future searches on similar objects. You can configure a filter definition tree only in flat maps. Once a filter is applied the name of the filter is displayed on the screen in the top-left, next to the filter icon. The filter definition tree form is launched by clicking on the Filter icon.

4.1.4 Map filtering

You can filter the IGP, OSPF, ISIS, and MPLS topology maps to reduce the number of objects that you are viewing. You can filter:

- **highlighted objects**

Choose one or more highlighted sessions and filter out objects that are not in the highlighted sessions. The filtered objects are faded or hidden.

- **IPv4 Route Targets**
  Highlight PEs advertising routes with certain RTs. You can hide or fade out the routers that are not highlighted.
- **object groups shown in flat map**
  Choose a group of objects and filter out all of the other objects. You can select routers, subnets, link groups, and links.

See 4.16 “To filter objects displayed on a topology map” (p. 66) and 4.17 “To filter highlighted objects displayed on a topology map” (p. 67) for information.

4.1.5 Suspended devices

When you need to exclude a device from CPAM management, but do not want to lose the CPAM information about the device, you can use a GUI or OSS client to suspend the management of the device. Once a device is suspended, SNMP communication fails. As a result, the following features cannot be used:

- Auto LSP Ping OAM
- Auto LSP Trace OAM
- Auto P2MP LSP Ping OAM
- Auto P2MP LSP Trace OAM
- Auto IP Path ICMP Ping OAM
- Auto IP Path ICMP Trace OAM
- LSP Active Path with LSP Ping
- P2MP Active Path with LSP Ping
- SDP of MPLS LDP Service Tunnel
- IP Path SPF with Ping
- Path Resource Audit
- OAM Multicast Tree

Both suspended devices and unreachable devices appear as purple on all CPAM topology maps. See “To manage, suspend, or unmanage a device” in the *NSP NFM-P Classic Management User Guide* for more information about suspended devices, including how to suspend device management.

4.1.6 CPAM span of control

For CPAM topology maps, the movement of objects on the map, and drag-and-drop management of groups and NEs, is disabled by default. To move and manage map objects, you must create a custom CPAM span of control, and select the required equipment group objects to add to that span. You must then add the custom CPAM span of control to the span of control profile for the required user group. There are no default CPAM spans. See the section on NFM-P user security in the *NSP System Administrator Guide* for more information about span of control.

The following CPAM topology map types support span of control:

- IGP topology
- OSPF topology
- OSPFv3 topology
- ISIS topology
- MPLS topology
- Multicast Manager topology

CPAM topology maps support span of control configuration only for the Equipment Group object type. In the context of CPAM span of control, the Equipment Group span object type corresponds to the groups on CPAM topology maps. The system-defined span objects are the system-defined groups in each map; for example, the OSPF or ISIS root group object, or the Discovered Vertices group object. User-defined groups are also available as span objects.

CPAM span of control supports equipment groups from the CPAM application only. Equipment groups from the CPAM Simulator application are not supported for span of control.

CPAM span of control supports only the Edit Access span type. View Access, Blocked View, and Blocked Edit spans are not supported. Span of control settings for CPAM objects do not affect the visibility of map objects; users can always view all CPAM topology map objects.

4.1.7 Workflow to configure span of control for CPAM topology maps

You must have the required administrative scope of command permissions to perform span of control configurations.

1

Create user-defined groups as required in CPAM topology maps; see 4.10 “To create user-defined groups on topology maps” (p. 62).

2

Create a custom span of control for CPAM that includes the required CPAM map groups; see the section on creating a span of control in the *NSP System Administrator Guide*.

During span of control configuration, you must choose Equipment Group as the object type from the Add menu on the Contents tab. On the Select Equipment Group – Span form, you can select system-defined or user-defined CPAM groups.

The selected groups are explicitly added to the span. Child objects of a group have the same edit access as the explicitly added group.

When selecting groups to add to the span (on the Select Equipment Group – Span form), you can sort or filter for CPAM groups using the Application column. You must choose CPAM as the application type, not CPAM Simulator.

3

Add the custom CPAM span to the required span of control profile for the user group; see the section on creating a span of control profile in the *NSP System Administrator Guide*.

When you add the custom CPAM span to the profile, you must choose Edit Access as the span type. The View Access, Blocked View, and Blocked Edit span types are not supported for CPAM.

4

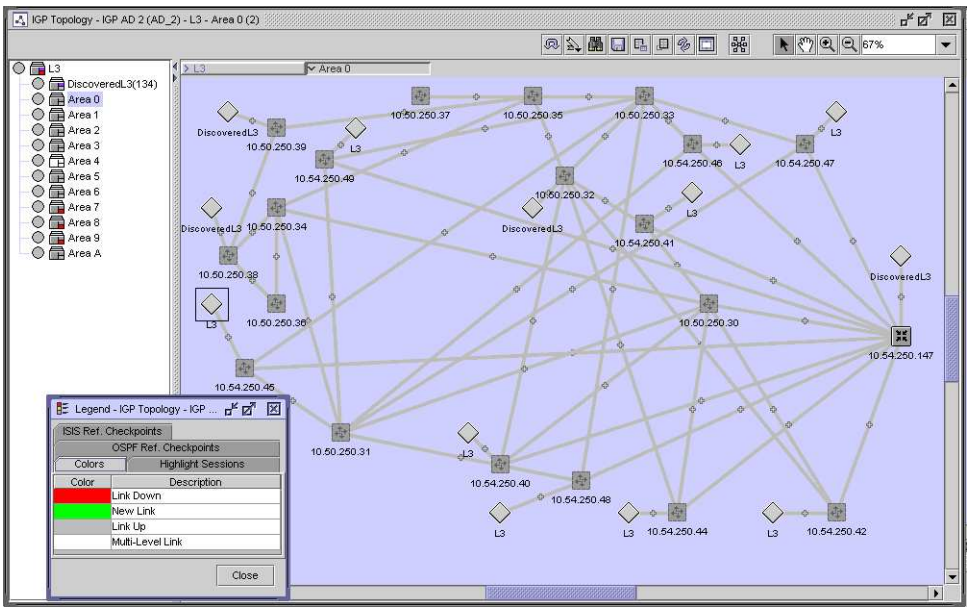
Ensure that the span of control profile with the CPAM span is assigned to the required user group; see the section on creating an NFM-P user group in the *NSP System Administrator Guide*.

4.2 IGP topology overview

4.2.1 Introduction to CPAM IGP topology

The IGP topology displays a combination of the ISIS and OSPF topologies on a map to provide a complete view of the IGP network. The following figure shows a sample IGP topology.

Figure 4-1 IGP topology



4.2.2 Routers

The following table lists the icons used by the CPAM to identify the roles of the routers in an IGP network.

Table 4-1 Router icons

Icon	IGP and MPLS Router Role
	Unmanaged router
	Managed router

You can navigate directly to a router if the router is being managed by the NFM-P. You can also use the following contextual menu options by right-clicking on the router icon:

- **Highlight Next Hop**

The Highlight Next Hop menu option opens the Next Hop form for the selected object (managed and unmanaged devices).

- **Resync**

  The Resync menu option specifies that SNMP MIB and CLI information bases are re-read to resynchronize them with the NFM-P, which also resynchronizes the network management settings with the router. Resynchronization does not affect the contents of the historical statistics database or LSDB information (managed devices only).

- **Equipment Manager**

  The Equipment Manager option launches the NFM-P equipment manager. The information for the selected managed device is displayed (managed devices only).

- **NE Sessions**

  The NE Sessions option opens a Telnet session, an SSH session, an FTP file browser session, or an SSH file browser session with the selected device (managed devices only).

- **NE Properties**

  The NE Properties option opens the network element property form for the selected object. This form displays read-only information and configurable parameters (managed devices only).

- **Properties**

  The Properties option opens the router property form for the selected object. This form displays read-only information and configurable parameters.

Devices that are not managed by the NFM-P are displayed with lighter-colored arrow icons than a managed device. There is no contextual menu for unmanaged devices.

4.2.3 Map visualization

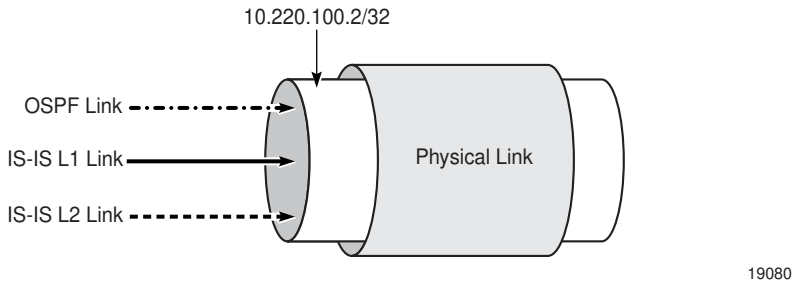
Protocol-specific information for an area, level, or router role does not appear on the map when you view a combined topology. The following display conditions are applied to the map for IGP topologies.

- The router icon displays the NFM-P management status for the router. The icon does not identify the role or ISIS area information for the router.
- The links are not colored by area or level. A link has a dark green color if it is operationally up, light green when it has been discovered by the system but has not yet had a checkpoint applied to it, red when it has had a checkpoint applied to it but is no longer seen by the system, and white when a group contains links with multiple colors.
- A circle icon represents OSPF transit networks and ISIS pseudonodes.

4.2.4 Protocols

You can configure several IGP protocols on the same link. The following figure shows an example of OSPF and ISIS running independently on the same link. The IGP map shows all of the links.

Figure 4-2 Multiple IGP links on an interface



Because each link can have another metric, SPF calculations vary depending on the protocol link used by the route. Link selection is specific to the router and varies depending on route policies, protocol weights, and other factors.

In cases where there are multiple protocols on a link, OSPF or ISIS is used in SPF calculations depending on the learned protocol for the destination address, as described in the following table:

Table 4-2 Protocol rules for SPF calculations

Protocol at source	Protocol at destination	Protocol used in SPF calculation
OSPF	OSPF	OSPF
ISIS	ISIS	ISIS
OSPF/ISIS	OSPF/ISIS	OSPF
OSPF	ISIS	ISIS
ISIS	OSPF	ISIS
OSPF	OSPF/ISIS	OSPF
OSPF/ISIS	ISIS	ISIS
OSPF/ISIS	OSPF	OSPF
ISIS	OSPF/ISIS	ISIS

4.2.5 Dot1 Q and QinQ

A physical link between two routers can have multiple IGP links when the interface is configured with Dot1Q or QinQ. Each logical link, in the case of Dot1 Q, must have a unique start and end IP address. Each of the logical links can be configured with OSPF, L1 ISIS, and L2 ISIS links.

Each link can advertise a different set of bandwidth parameters when you enable the respective traffic engineering protocol. The bandwidth parameters do not assess other links from the same or different protocols because OSPF and ISIS protocols have no view of the physical layer.

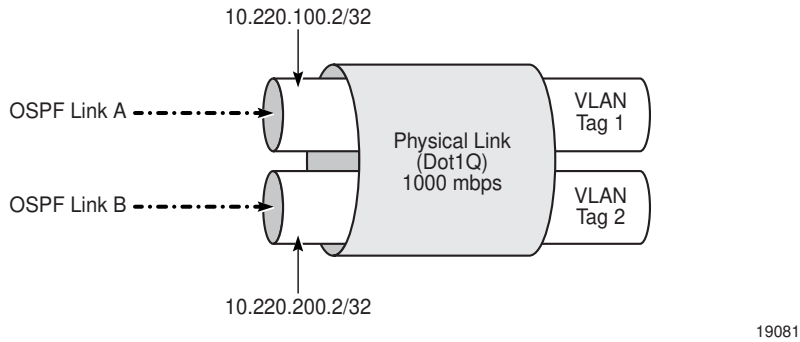
Figure 4-3, “Multiple interfaces on the same physical link” (p. 48) shows a physical link that is configured to use Dot1 Q with 1000 Mb/s. Two network interfaces are created:

- **Interface A (configured for OSPF)**

10.220.100.2/32 using VLAN tag of 1

- **Interface B (configured for OSPF)**
  10.220.200.2/32 using VLAN tag of 2

Figure 4-3 Multiple interfaces on the same physical link



The example displayed in Figure 4-3, “Multiple interfaces on the same physical link” (p. 48) also applies to any combination of OSPF and ISIS links running on the same physical link.

The following table lists the bandwidths that are initially advertised by the OSPF-TE protocol.

Table 4-3 Initial bandwidth for links

Link	Available bandwidth (Mb/s)
OSPF Link A	1000
OSPF Link B	1000
Physical link	1000

The bandwidth for the physical link is reduced to 750 Mb/s if an LSP crossing interface A (10.220.100.2/32) reserves 250 Mb/s of bandwidth. The effective bandwidth is reduced to 750 Mb/s on only OSPF Link A because OSPF-TE has no concept of physical links. The bandwidth is not affected on OSPF Link B. The following table describes the bandwidth that is available on the links:

Table 4-4 Reserved bandwidth for links

Link	Available bandwidth (Mb/s)
OSPF Link A	750
OSPF Link B	1000
Physical link	750

A system that uses bandwidth and performs bandwidth reservation tasks such as the ABM must be aware of conditions when multiple IGP links traverse the same the physical link.

4.2.6 Non-routed edge discovery

Non-routed edge discovery policies allow you to discover non-routed interfaces and subnets and represent them as adjacencies on the CPAM IGP and MPLS topology maps. A non-routed edge discovery policy requires a specified set of aggregator and edge NEs, and discovers static routes and subnets by using the routing interfaces of the specified NEs. See 4.25 “To configure a non-routed edge discovery policy” (p. 73) for more information about configuring a non-routed edge discovery policy.

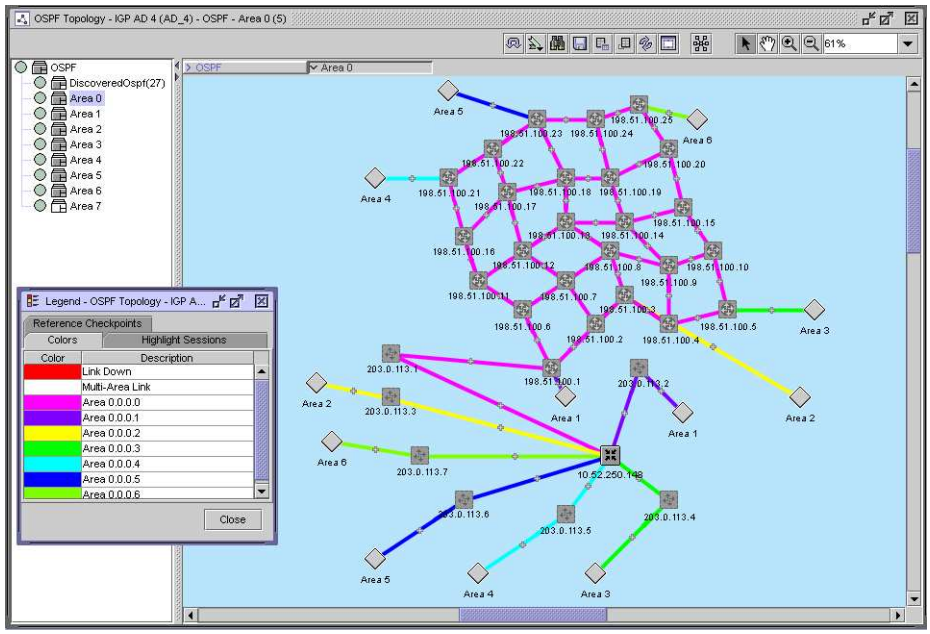
4.3 OSPF topology overview

4.3.1 Introduction to CPAM OSPF topology

The OSPF-TE topology map displays all of the OSPF-enabled routers and OSPF links that are discovered by the CPAAs. The discovery is independent of the discovery of routers that are managed or manageable by the NFM-P.

The following figure displays a discovered OSPF network with six routing areas. The CPAA with the IP address 10.52.250.148 is connected to 6 areas, and the backbone.

Figure 4-4 OSPF view



4.3.2 Routers

The following table lists the icons used by the CPAM to identify the roles of the routers in a routing area.

Table 4-5 Router icons

Icon	OSPF Router role
	ASBR/Internal
	ABR
	ASBR/ABR
	Network (subnet)
	Unmanaged router
	Managed internal router
	Unmanaged ABR
	Unmanaged ASBR/ABR

You can navigate directly to a router if the router is currently managed by the NFM-P. You can also use the following contextual menu options by right-clicking on the router icon:

- **Select Attached**
  The Select Attached menu option selects routers that are attached to the selected object.
- **Layout Selected**
  The Layout Selected menu option specifies the layout of the router on the topology map (circular or smart organic).
- **Fade Out Others**
  The Fade Out Others menu option fades out all of the objects on the map except for the selected router. You can cancel the fade out by choosing Cancel Fade Out from the contextual menu.
- **Show Only Selected**
  The Show Only Selected menu option hides all of the objects on the map except for the selected router. You can cancel the hide operation by choosing Cancel Show Only from the contextual menu.
- **Resync**

The Resync menu option specifies that SNMP MIB and CLI information bases are re-read to resynchronize them with the NFM-P, which also resynchronizes the network management settings with the router. Resynchronization does not affect the contents of the historical statistics database or LSDB information (managed devices only).

- **Equipment Window**

  The Equipment Window option launches the NFM-P equipment window. The information for the selected managed device is displayed (managed devices only).

- **NE Sessions**

  The NE Sessions option opens a Telnet session, an SSH session, an FTP file browser session, or an SSH file browser session with the selected device (managed devices only).

- **Scripts**

  The Scripts options opens the script manager form for the selected object. This form displays any scripts that are associated with the object.

- **NE Properties**

  The NE Properties option opens the network element property form for the selected object. This form displays read-only information and configurable parameters (managed devices only).

- **BGP**

  The BGP option allows you to run a CLI script to view BGP routes for the router, or to show BGP paths for the router.

- **Properties**

  The Properties option opens the router property form for the selected object. This form displays read-only information and configurable parameters.

- **Synchronize Groups on Selected Routers**

  The Synchronize Groups on Selected Routers option verifies if an equipment group exists on the physical map and creates a group on the CPAM to which the selected router or routers are moved.

Devices that are not managed by the NFM-P are displayed with lighter-colored arrow icons than a managed device. There is no contextual menu for unmanaged devices.

4.3.3 Subnet objects

The subnet object represents the transit network and is displayed as a small circle icon on the topology map. The subnet object also identifies the network IP address and the prefix length, for example, 10.220.219.1/24.

Broadcast multi-access networks, such as Ethernet networks, use a DR to prevent each router on the network from forming a link with all of the other routers on the same broadcast network. A BDR is also selected in the event the DR is down. There is no specific representation of a DR or BDR on the topology map.

The DR information for a subnet is available on the property form for the transit network object.

4.3.4 Links

The CPAM supports the following OSPF links:

- point-to-point

- broadcast
- virtual

A point-to-point OSPF link is a logical unidirectional link between OSPF interfaces.

For OSPF links in a broadcast subnet, the link begins on the first router and terminates on a subnetwork. There is a duplicate link in the opposite direction, from the subnetwork to another router. The duplicate link always has a metric and bandwidth of 0. Broadcast links are used when the routers are connected using an Ethernet network (hub or switch). A circle icon identifies Ethernet subnetwork configurations. A broadcast link uses one endpoint as a subnet and one endpoint as an OSPF interface of a router.

The CPAM does not support non-broadcast multi-access links, such as frame relay or X.25.

The direction of a unidirectional OSPF link is indicated by an arrow on the map. Two links between two interfaces are grouped into one link with no indication of direction. All of the links between two routers are grouped into one link group.

OSPF virtual links are represented as very thin lines on the map. The CPAA cannot be an endpoint of a virtual link.

The links contain additional bandwidth-related parameters if OSPF-TE is enabled in the OSPF network, and if the router is enabled with OSPF-TE.

4.3.5 Routing areas

Routing areas are identified on the topology map by the colors of the links. Each area is represented with another color. Links that belong to the same routing area are the same color. See Chapter 18, “Impact analysis” for information about color variations for links within the same area. See 4.19 “To configure link colors for OSPF areas or ISIS instances” (p. 68) for information about configuring link colors.

If a routing area is not connected to a CPAA, the CPAM does not know the routing area topology.

4.3.6 LSDB updates

You can retrieve the LSDB information from the CPAA to the database. See 4.9 “To update the LSDB” (p. 62) for information.

If you enable the OSPF protocol events flag of the CPAA, the CPAM ensures that the LSDB is up to date by using the following rules:

- When the CPAA becomes operationally up and OSPF events are currently enabled, the CPAM automatically retrieves the LSDB. This includes the start-up time of the CPAM.
- When the CPAA is already operationally up and OSPF events become enabled, the CPAM automatically retrieves the LSDB.

Router and network LSAs that are received by a CPAA are forwarded to the CPAM. A timestamp is added to each entry to facilitate future RCA. See Chapter 14, “Root cause analysis” for information about the CPAM and RCA.

4.3.7 SRLG

A set of links can be considered a shared risk link group if they share a resource whose failure may affect all of the links in the set. A link can belong to multiple SRLGs. An SRLG is identified by a 32-bit number that is unique within an IGP domain.

OSPF TE extensions for SRLG

The SRLG values are carried in sub-TLV 16 of the Link TLV in OSPF TE extensions. You can view the value of the SRLGs to which the link belongs on the Shared Link Risk Group tab of OSPF links.

When the IGP topology is checkpointed, the SRLG values are also recorded. When two checkpointed links are compared, the SRLG values are also compared between the two instances and changes are reported in the result.

4.4 OSPFv3 topology overview

4.4.1 Introduction to CPAM OSPFv3 topology

The OSPFv3 topology map displays all of the OSPFv3-enabled routers and OSPFv3 links that are discovered by the CPAAs. The discovery is independent of the discovery of routers that are managed or manageable by the NFM-P.

4.4.2 Routers

See 4.3.2 “Routers” (p. 49) in the 4.3 “OSPF topology overview” (p. 49) section for information about routing icons and contextual menu options on the OSPFv3 topology map.

4.4.3 Subnet objects

See 4.3.3 “Subnet objects” (p. 51) in the 4.3 “OSPF topology overview” (p. 49) section for information about subnet objects on the OSPFv3 topology map.

4.4.4 Links

The CPAM supports the following OSPFv3 links:

- point-to-point
- broadcast
- virtual

A point-to-point OSPFv3 link is a logical unidirectional link between OSPFv3 interfaces.

For OSPFv3 links in a broadcast subnet, the link begins on the first router and terminates on a subnetwork. There is a duplicate link in the opposite direction, from the subnetwork to another router. The duplicate link always has a metric and bandwidth of 0. Broadcast links are used when the routers are connected using an Ethernet network (hub or switch). A circle icon identifies Ethernet subnetwork configurations. A broadcast link uses one endpoint as a subnet and one endpoint as an OSPFv3 interface of a router.

The CPAM does not support non-broadcast multi-access links, such as frame relay or X.25.

The direction of a unidirectional OSPFv3 link is indicated by an arrow on the map. Two links between two interfaces are grouped into one link with no indication of direction. All of the links between two routers are grouped into one link group.

OSPFv3 virtual links are represented as very thin lines on the map. The CPAA cannot be an endpoint of a virtual link.

4.4.5 Routing areas

See 4.3.5 “Routing areas” (p. 52) in the 4.3 “OSPF topology overview” (p. 49) section for information about routing areas on the OSPFv3 topology map.

4.4.6 LSDB updates

You can retrieve the LSDB information from the CPAA to the database. See 4.9 “To update the LSDB” (p. 62) for information.

If you enable the OSPFv3 protocol events flag of the CPAA, the CPAM ensures that the LSDB is up to date by using the following rules.

- When the CPAA becomes operationally up and OSPFv3 events are currently enabled, the CPAM automatically retrieves the LSDB. This includes the start-up time of the CPAM.
- When the CPAA is already operationally up and OSPFv3 events become enabled, the CPAM automatically retrieves the LSDB.

Router and network LSAs that are received by a CPAA are forwarded to the CPAM. A timestamp is added to each entry to facilitate future RCA. See Chapter 14, “Root cause analysis” for information about the CPAM and RCA.

4.5 ISIS topology overview

4.5.1 Introduction to CPAM ISIS topology

The ISIS topology map displays all of the routers and ISIS links that are detected by the CPAAs. All of the NFM-P-managed and -manageable routers are displayed.

You can configure multiple ISIS instances on a CPAA. A CPAA can monitor up to 32 ISIS L1 routing domains and the ISIS backbone (L2 domain). The L2 adjacency can be established only in the instance 0. By default, all of the other instances are L1-capable only. Each ISIS L1 domain should have an adjacency to only one CPAA. You can add each ISIS interface to one instance.

The ISIS area ID for each CPAA ISIS instance must be unique in the IGP administrative domain.

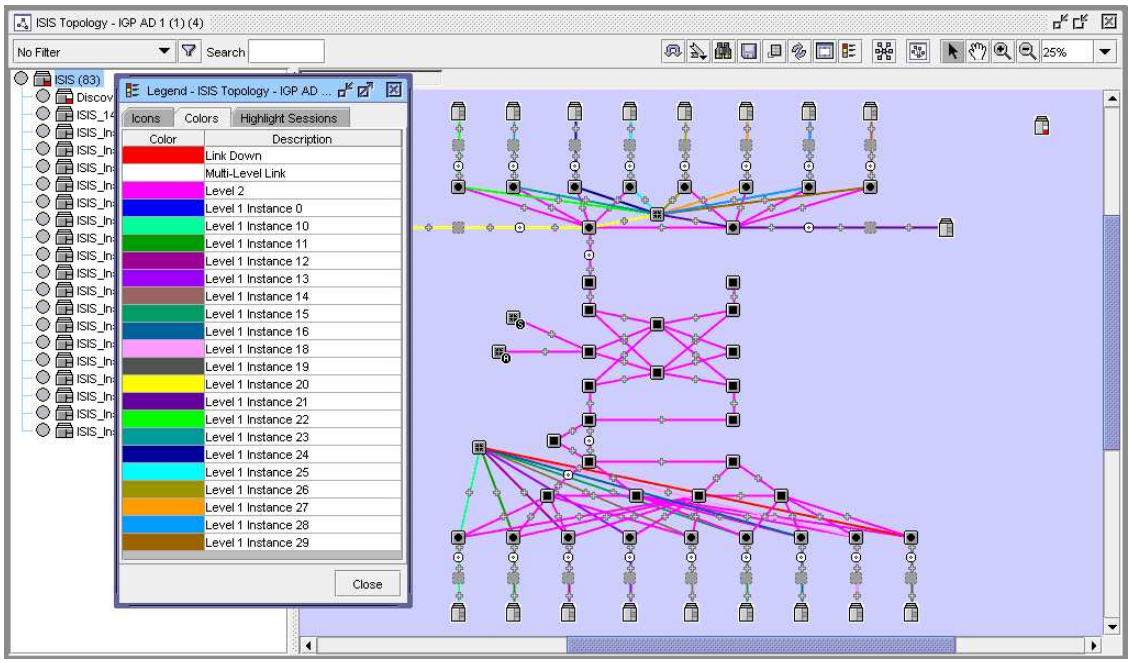
If the network architecture includes Area IDs that are the same, a new Area ID that is unused in the network should be created between the CPAA instance and the connected router. If Area IDs are not unique, the CPAA configuration should be changed prior to an upgrade.

The CPAM uses the area ID to identify different L1 domains on the map with different colours. Although the routers in the L1 domain can have more than one area ID, or another area ID from the CPAA, the entire L1 domain is identified by the CPAA area ID on the map.

Instance numbers and Area IDs should be identical for a redundant CPAA pair.

The following figure shows a discovered ISIS network with multiple level 1 instances and one level 2 instance.

Figure 4-5 ISIS view



4.5.2 Routers

The following table lists the icons used by the CPAM to identify the roles of the routers in a routing area.

Table 4-6 Router icons

Icon	ISIS Router role
	L1-L2
	Network (subnet)
	Unmanaged L1

Table 4-6 Router icons (continued)

Icon	ISIS Router role
	Managed L1
	Unmanaged L1-L2
	Unmanaged L2
	L2

Broadcast multi-access networks, such as Ethernet networks, use a DR to prevent each router from forming a link with every router in an Ethernet network.

The CPAM uses the router ID as the identifier of a router. Routing protocol instances, such as IGP, must share the same router ID.

Note: In a standard ISIS, because the protocol operates using system IDs, there is no method to easily determine the router ID. The TE router ID is available when you configure the traffic engineering extension.

When assigning a Router ID to an ISIS router with no TE router ID, the assigned Router ID should be a reachable IP address (via ISIS) on the node.

With 7450 ESS and 7750 SR service routers, the router ID is always available in the LSP regardless of the traffic engineering configuration. Although the system ID, system IP address, and router ID may differ, the router ID is the system IP address by default.
The following restrictions apply to ISIS SPF calculations, next hop configurations, and topology map highlighting:

- Full support for SPF and managed routes is available when the TE router ID is included in the protocol.
- ISIS systems without a TE router ID can be detected by the CPAM but will not be shown on the topology map until a TE router ID is assigned.

You can navigate directly to a router if the router is currently managed by the NFM-P. You can also use the following contextual menu options by right-clicking on the router icon:

- **Highlight Next Hop**
  The Highlight Next Hop menu option opens the Next Hop form for the selected object (managed and unmanaged devices).
- **NE Sessions**
  The NE Sessions option opens a Telnet session, an SSH session, an FTP file browser session, or an SSH file browser session with the selected device (managed devices only).
- **Properties**

The Properties option opens the router property form for the selected object. This form displays read-only information and configurable parameters.

4.5.3 Subnet objects

The subnet object represents a pseudonode in the ISIS network and appears as a small circle icon on the map. The subnet object displays the system ID and pseudonode ID of the subnet, for example, 0100.0118.2213-04.

Broadcast multi-access networks, such as Ethernet networks, use a DR to prevent each router on the network from forming a link with all of the routers on the same broadcast network. There is no specific identifier for a DR on the map.

The DR information for a subnet is available on the property form for the pseudonode subnet object.

4.5.4 Links

The CPAM supports the following ISIS links:

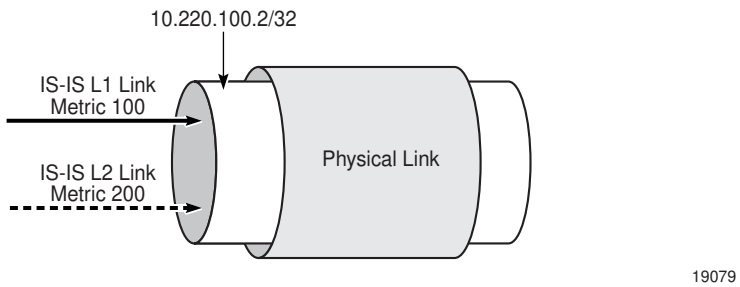
- point-to-point
- broadcast

Point-to-point links directly connect two adjacent routers. Broadcast links are used when the routers are connected using an Ethernet or token ring network (hub or switch). The CPAM uses a circle on the topology map to identify a subnet, or pseudonode. A broadcast link always has one endpoint as a circle and one endpoint as an ISIS interface of a router. When you create a link from a router to a network, the CPAM creates a duplicate link in the reverse direction. The duplicate link always has a metric and bandwidth of 0.

The CPAM does not support non-broadcast multi-access links, such as frame relay or X.25.

An ISIS link under the CPAM can be designated as a Level 1 or Level 2 link, but not both at the same time. The CPAM creates two different links if there is a Level 1 and Level 2 adjacency between two ISIS interfaces. The figure below shows an example of the ISIS adjacency configuration. The different links support the unique metrics that you can configure for each level. For SPF calculations, if there are both L1 and L2 links, the determination of the active link is dependent on whether the destination address is local or external to the L1 area.

Figure 4-6 ISIS Level 1 and Level 2 links



An ISIS link is a level-specific (L1 or L2) connection from an ISIS interface to the following network components:

- ISIS interface (point-to-point)
- pseudonode network (broadcast network)

The map uses an arrow to display the direction of a unidirectional ISIS. Two links between two interfaces are grouped, by default, as one link with no defined direction. By default, all of the links between two routers are grouped into one link group.

4.5.5 Router support for ISIS-TE Neighbor TLV

Router support for ISIS-TE Neighbor TLV determines the level of support the routing analyzer provides for the parallel links between interfaces. In a standard ISIS, only one neighbor is advertised even if there are parallel links between the neighbors. The TE Neighbor TLV contains all of the parallel links and the IP addresses configured on each terminating interface. This configuration allows the routing analyzer to create the parallel links, and in the case of managed routers, provide navigation to the NFM-P ISIS interface.

In the 7750 SR amd 7450 ESS, the ISIS protocol advertises the ISIS-TE Neighbor TLV even if ISIS-TE is not enabled. Bandwidth-related TLVs are advertised to the network when you enable ISIS-TE. This functionality is not common to all of the devices. You must enable ISIS-TE for devices that do not support unconditional advertising of the TE Neighbor TLV.

4.5.6 ISIS L1 routing domain

The L1 routing domain is equivalent to a non-backbone OSPF routing area. An L1 routing domain can contain routers with one or more defined area IDs. In addition, two routers belonging to two different L1 routing domains can use the same routing area. A CPAA can be connected to only one L1 routing domain.

4.5.7 LSDB updates

Each Link State PDU (LSP) received by a CPAA is forwarded to the CPAM. In ISIS there is no distinction between router and network LSPs, with the following exceptions:

- router-based LSPs contain a PSN of 0
- network LSPs have a non-zero PSN

You can retrieve the LSDB from the CPAA to the database. See 4.9 “To update the LSDB” (p. 62) for information.

If you enable the CPAA ISIS protocol events flag, the CPAM ensures that the LSDB is up to date by using the following rules.

- When the CPAA becomes operationally up and ISIS events are currently enabled, the CPAM automatically retrieves the LSDB. This includes the start-up time of the CPAM.
- When the CPAA is already operationally up and ISIS events become enabled, the CPAM automatically retrieves the LSDB.

4.5.8 SRLG

A set of links can be considered a shared risk link group if they share a resource whose failure may affect all of the links in the set. A link can belong to multiple SRLGs. An SRLG is identified by a 32-bit number that is unique within an IGP domain.

ISIS TE extensions for SRLG

The SRLG values are carried in sub-TLV 16 of the Link TLV in ISIS TE extensions. You can view the value of the SRLGs to which the link belongs on the Shared Link Risk Group tab of ISIS link.

When the IGP topology is checkpointed, the SRLG values are also recorded. When two checkpointed links are compared, the SRLG values are also compared between the two instances and changes are reported in the result.

4.6 Topology map management workflow

4.6.1 Stages

1

Determine the map type you want to view.

- maps that show IGP topology
- maps that show protocol-specific topologies

See 4.7 “To open a topology map from the NFM-P main menu” (p. 61) for more information.

2

View the relationship between objects drawn on the map.

3

Manage checkpoints. See Chapter 18, “Impact analysis” for more information.

4

Update the LSDB, if required. See 4.9 “To update the LSDB” (p. 62) for more information.

5

Create topology map groups, as required. See 4.10 “To create user-defined groups on topology maps” (p. 62) for more information.

6

Synchronize the IGP topology map with the NFM-P physical topology map, or synchronize the OPSF, OSPFv3, or ISIS topology map with the IGP topology map. See 4.11 “To synchronize topology maps” (p. 63) for more information.

7

Assign a router ID to an ISIS router with no TE router ID when the TopologyIsisSystemError alarm is raised, as required. See 4.12 “To assign a router ID to ISIS routers with no TE router ID” (p. 63) for more information.

8

Open a flat map, if required. See 4.13 “To open a flat map” (p. 64) for more information.

9

Manage filters for flat topology maps, if required:

1. Create a filter for the flat map. See 4.14 “To create a filter for flat maps” (p. 65) for more information.
2. Apply a filter to the flat map. See 4.15 “To apply a filter to a flat topology map” (p. 65) for more information.

10

Filter and list objects on topology maps, if required:

1. Filter the objects displayed on the topology map. See 4.16 “To filter objects displayed on a topology map” (p. 66) for more information.
2. Filter the highlighted objects displayed on the topology map. See 4.17 “To filter highlighted objects displayed on a topology map” (p. 67) for more information.
3. Remove selected references displayed on the topology map. See 4.18 “To remove specific references displayed on a topology map” (p. 68) for more information.
4. List objects displayed on the topology map using a specific link. See 4.20 “To list objects using a selected link” (p. 69) for more information.
5. List or view object information for objects displayed on the topology map. See 4.21 “To list or view object information from a map” (p. 70) for more information.

11

View the legend information, if required. See 4.22 “To view the legends for a topology map” (p. 71) .

12

Configure the type of information that is displayed on the CPAM topology map icon labels, if required. See 4.23 “To configure and view CPAM topology map icon labels” (p. 71) for more information.

13

Configure the available menu options for IGP administrative domains, if required. See 4.24 “To configure available menu options for IGP administrative domains” (p. 72) for more information.

14

Configure non-routed edge discovery policies to discover non-routed interfaces and subnets and represent them as adjacencies on the CPAM IGP and MPLS topology maps, if required. See 4.25 “To configure a non-routed edge discovery policy” (p. 73) for more information.

15

Override non-routed edge discovery policies for specific routing interfaces to prevent network interfaces from being included in discovery calculations and from appearing on topology maps, if required. See 4.26 “To override a non-routed edge discovery policy for a routing interface” (p. 74) for more information.

4.7 To open a topology map from the NFM-P main menu

4.7.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The topology map opens.

2

Close the topology map.

END OF STEPS

4.8 To configure topology window overlay type from the NFM-P main menu

4.8.1 Steps

1

Choose Application→User preferences from the NFM-P main menu. The User Preferences form opens.

2

Configure the Overlay Type parameter.

3

Close the form.

END OF STEPS

4.9 To update the LSDB

4.9.1 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.

2

Choose CPAA (CPAM: Topology) and click Search.

3

Choose an entry and click Properties. The CPAA (Edit) form opens.

4

Perform one of the following:

a. Click Retrieve from CPAA, then choose OSPF LSDB to retrieve OSPF routing data for the CPAA.

b. Click Retrieve from CPAA, then choose ISIS LSDB to retrieve ISIS routing data for the CPAA.

5

Perform one of the following steps to ensure real-time updates:

a. Enable the OSPF/OSPF-TE option of the Event Types parameter.

b. Enable the ISIS/ISIS-TE option of the Event Types parameter.

6

Close the forms.

END OF STEPS

4.10 To create user-defined groups on topology maps

4.10.1 Steps

1

Choose Tools→Route Analysis→*Topology_type* from the NFM-P main menu. The topology map opens.

2

Right-click on the topology map area and choose Create Group. The Group (Create) form opens.

3

Configure the required parameters.

4

Close the form.

End of steps

4.11 To synchronize topology maps

4.11.1 General information

The CPAM IGP topology map can be synchronized with the NFM-P physical map to provide consistent organization of managed and unmanaged routers, and groups. The OSPF, OSPFv3, and ISIS topology maps can be synchronized with the IGP topology map.

4.11.2 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_administrative_domain* from the NFM-P main menu. The topology map opens.

2

As required, right-click on the topology map and choose Sync Tools→Initialize View to clear any existing configurations.

3

Perform one of the following:

a. On the IGP topology map, right-click and choose Sync Tools→Sync map with the physical map.

Note: Changes made to the IGP administrative domain will be reflected on Multicast and MPLS topologies.

b. On the OSPF, OSPFv3, or ISIS topology map, right-click and choose Sync Tools→Sync map with the IGP map.

End of steps

4.12 To assign a router ID to ISIS routers with no TE router ID

4.12.1 When to use

Perform this procedure to assign a router ID to an ISIS router with no TE router ID when the TopologyIsisSystemError alarm is raised by the CPAM.

4.12.2 Steps

1

Choose Tools→Route Analysis→IGP Network Data from the NFM-P main menu. The IGP Network Data form opens.

2

Choose ISIS System ID Mapping (CPAM: Topology) and click Search.

3

Choose an entry and click Properties. The ISIS System ID Mapping (Edit) form opens.

4

Configure the Router ID parameter.

Note: The Router ID should be an IP address that is reachable (via ISIS) on the node.

5

Save your changes and close the forms.

END OF STEPS

4.13 To open a flat map

4.13.1 Steps

1

Choose Tools→Route Analysis→Flat Maps→*Topology_type*→*IGP_administrative_domain* from the NFM-P main menu. The Topology Filter - *Topology_type* - Flat window opens.

2

Perform one of the following:

a. Create a new filter. See 4.14 “To create a filter for flat maps” (p. 65) .

b. Select an existing filter. Continue to Step 3 .

3

Click Load. The Topology Filter form opens.

4

Click Search.

5

Choose a filter and click OK. The Filter -*(object)* window opens.

6

Save your changes and close the forms.

End of steps

4.14 To create a filter for flat maps

4.14.1 General information

The filter allows you to create a filtered list of objects in a flat map. You configure the filter to quickly view specific objects. You can save the filter to use for similar searches on similar objects.

4.14.2 Steps

1

Open a flat map. See 4.13 “To open a flat map” (p. 64) .

2

Choose an object and click Add object filter.

3

Configure the filter and click Save. The Save Filter form opens.

4

Configure the required parameters.

5

Save your changes and close the forms.

End of steps

4.15 To apply a filter to a flat topology map

4.15.1 General information

See 4.14 “To create a filter for flat maps” (p. 65) for information about creating a filter definition tree.

4.15.2 Steps

1

Open a flat map. See 4.13 “To open a flat map” (p. 64) .

2

Click on the filter icon. The Filter Tree - *(object)* Topology - Flat form opens.

3

Click Load. The Select window opens.

4

Choose a filter and click OK. The Filter Tree - *(object)* Topology - Flat window opens.

5

Click Build View.

6

Click OK to confirm.

END OF STEPS

4.16 To filter objects displayed on a topology map

4.16.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The topology map opens.

2

Select one or more objects and perform one of the following:

a. To hide all of the objects on the topology map except for the selected objects, go to Step 3 .

b. To fade objects on the topology map except for the selected objects, go to Step 4 .

3

Right-click on the topology map and choose Show Only Selected. Go to Step 5 .

4

Right-click on the topology map and choose Fade Out Others.

5

To cancel the operation, perform one of the following:

a. Right-click on the topology map and choose Cancel Show Only.

b. Right-click on the topology map and choose Cancel Fade Out.

End of steps

4.17 To filter highlighted objects displayed on a topology map

4.17.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The topology map opens.

2

Right-click on the topology map and choose Highlight Sessions. The Highlight Sessions window opens.

3

Perform one of the following:

a. To hide all of the objects on the topology map except for the highlighted objects, go to Step 4 .

b. To fade objects on the topology map except for the highlighted objects, go to Step 5 .

4

Right-click on the highlight session entry and choose Show Only Highlighted. Go to Step 6 .

5

Right-click on the topology map and choose Fade Out Others.

6

To cancel the operation, perform one of the following:

a. Right-click on the highlight session entry and choose Cancel Show Only Highlighted.

b. Right-click on the topology map and choose Cancel Fade Out.

7

Close the Highlight Sessions window.

End of steps

4.18 To remove specific references displayed on a topology map

4.18.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The topology map opens.

2

Select a maximum of 20 references on the topology map.

Note: Subnets and bi-directional links must each be calculated individually when selecting multiple references for removal.

3

Right-click on the topology map and choose Cleanup Selected References.

Note: Changes made to the IGP administrative domain will be reflected on Multicast and MPLS topologies.

END OF STEPS

4.19 To configure link colors for OSPF areas or ISIS instances

4.19.1 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.

2

Choose Administrative Domain (CPAM: Topology) and click Search.

3

Choose an entry and click on the Properties button. The IGP Administrative Domain (Edit) form opens.

4

Click on the Color tab.

5

Click on the OSPFv2, OSPFv3, and ISIS tabs, as required.

6

Perform one of the following:

a. Choose an existing OSPF area or ISIS instance and click on the Properties button. The Color (Edit) form opens.

b. Click on the Create button. The Color (Create) form opens.

7

Configure the Name and Description parameters.

8

Configure the domain-specific parameters.

For ISIS domains, the System Instance ID parameter is configurable when the Level parameter is set to Level 1.

9

Perform one of the following:

a. Configure the Color Index parameter. Go to Step 11 .

b. Click on the Suggest button. An unused color or the least-used color is selected. Go to Step 11 .

c. Click on the Select button. The Choose color form opens.

10

Choose a color and click on the OK button. The form closes.

11

Save your changes and close the forms.

END OF STEPS

4.20 To list objects using a selected link

4.20.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The topology map opens.

2

Right-click on an expanded link and choose List Objects Using this Link. The List Objects Using this Link form opens.

Note: To expand a link group, right-click on a link group and choose Expand Group.

3

Click on any of the following tabs:

- IP Path Monitors—to view IP path monitors whose last record includes the segment on the selected IGP link
- Dynamic LSPs—to view dynamic LSPs whose last monitored record has the selected IGP link as one segment. Only LSPs that are being monitored are listed.
- Service Tunnels—to view service tunnels using the link
- Services—to view services using the link
- Composite Services—to view composite services using the link

4

Close the form.

END OF STEPS

4.21 To list or view object information from a map

4.21.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The topology map opens.

2

Right-click on one of the following objects:

- device icon
- plus sign icon in the center of a link or link group
- port of a custom node that indicates the endpoint of a link, path, tunnel, or service
- equipment group icon

3

Click on any of the following options, depending on the object selected in Step 2 :

- View a list of network objects, for example, the service tunnels of LSPs running in the group. You can then choose one and view or edit the configuration.
- Create new connections between the devices, as appropriate
- View the properties of the object. You can then view or edit the device configuration.

END OF STEPS

4.22 To view the legends for a topology map

4.22.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The topology map opens.

2

Perform one of the following:

a. Click the Legend button at the top of the topology map and choose Colors Legend. The Legend - *Topology_type* - *IGP_Administrative_Domain* form opens.

b. Click the Legend button at the top of the topology map and choose Icon Legend. The Legend - *Topology_type* - *IGP_Administrative_Domain* form opens.

3

Close the form.

END OF STEPS

4.23 To configure and view CPAM topology map icon labels

4.23.1 General information

You can configure the type of information you need to be displayed on the CPAM topology map icon labels.

4.23.2 Steps

1

Choose Application→User Preferences from the NFM-P main menu. The User Preferences form opens.

2

Click on the Topology tab.

3

Select one of the following topology map icons:

- CPAM Subnets
- CPAM Routers
- CPAM Simulated Routers
- CPAM Simulated Subnets

4

Configure Text Field #1 and Text Field #2 to identify the information you need to display in each map icon label. You can choose one of the following for each text field:

- CPAM Subnets and CPAM Simulated Subnets
  - Description
- CPAM Routers and CPAM Simulated Routers
  - Name
  - Management IP Address
  - Network Element Name
  - Description
  - Router ID
  - CPAM Name

Note: Choose CPAM Name to display the NE name for all of the SNMP-polled NEs and GNEs. The displayed name for an NE is:

- the managed NE name for fully managed NEs
- the ISIS protocol name for ISIS-supported NEs if an NE is unmanaged
- "N/A" if an NE is both unmanaged and non- ISIS-supported

5

Save your changes and close the form.

END OF STEPS

4.24 To configure available menu options for IGP administrative domains

4.24.1 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu.

2

Expand the Administrative Domain (CPAM: Topology) object and choose IGP Administrative Domain (CPAM: Topology).

3

Click Search.

4

Choose an entry and click Properties. The IGP Administrative Domain (Edit) form opens.

5

Configure the Enabled Menus parameter.

6

Save your changes and close the form.

END OF STEPS

4.25 To configure a non-routed edge discovery policy

4.25.1 General information

The following restrictions apply for configuring a non-routed edge discovery policy:

- NEs cannot be specified as aggregator nodes in more than one policy
- NEs that are specified as aggregators cannot be specified as edge nodes in the same or another policy
- NEs cannot be included in policies across admin domains

Note: A non-routed edge discovery policy does not automatically distinguish between routed and non-routed adjacencies, therefore operator intervention is required in order to prevent the inclusion of adjacencies that are already included in a routing protocol. You can use overrides to exclude specific routing interfaces from non-routed edge discovery policies in order to prevent routed adjacencies from being misrepresented on the topology maps. See 4.26 “To override a non-routed edge discovery policy for a routing interface” (p. 74) for more information.

4.25.2 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.

2

Choose Administrative Domain (CPAM: Topology) and click Search.

3

Choose an entry and click Properties. The IGP Administrative Domain (Edit) form opens.

4

Click on the Non-Routed Edge Discovery Policies tab.

5

Click Create. The Non-Routed Edge Discovery Policy (Create) form opens.

6

Configure the required parameters.

7

Specify aggregator routers and edge routers:

1. Click on the Aggregator Routers and Edge Routers tabs.
2. Click Add. A form opens.
3. Click Search.
4. Choose one or more entries and click OK. The form closes.

8

Save your changes and close the forms.

END OF STEPS

4.26 To override a non-routed edge discovery policy for a routing interface

4.26.1 General information

You can override non-routed edge discovery policies for specific routing interfaces in order to prevent network interfaces from being included in discovery calculations and from appearing on topology maps.

4.26.2 Steps

1

Choose one of the following.

a. Navigate to a routing interface from the navigation tree:
   1. Choose Routing from the navigation tree view selector.
   2. On the navigation tree, expand Network→Router→Routing Instance.
   3. Right-click on a routing interface object and choose Properties. The Network Interface (Edit) form opens.

b. Navigate to a routing interface by using an object manager:
   1. Choose Manage→Networking→Routing Instances from the NFM-P main menu. The Manage Routing Instances form opens.
   2. Choose Network Interface (Routing Management: General) and click Search.
   3. Choose an entry and click Properties. The Network Interface (Edit) form opens.

2

Configure the Show Link In IGP Topology parameter.

3

Save your changes and close the forms.

END OF STEPS

5 MPLS topology management

5.1 MPLS topology overview

5.1.1 Introduction to MPLS topology

In addition to IGP links, the MPLS topology map displays all of the MPLS, RSVP, and LDP interfaces for routers that are natively managed by the NFM-P. The MPLS topology map relies on IGP connectivity to determine which two RSVP or LDP interfaces are linked together. Because an operationally up RSVP-LDP interface link may not be functional if the IGP link is operationally down, the MPLS topology map displays IGP links to identify this problem.

When RSVP, LDP, and IGP interfaces are configured on a network interface, the IGP link can be operationally down while the other two interfaces are operationally up. In this case, the IGP link is not displayed on the MPLS topology but the RSVP and LDP interfaces appear. Because the connectivity of RSVP and LDP links rely on the missing IGP link, the RSVP and LDP interfaces from router X and Y are not connected.

Note: The CPAM MPLS topology view does not show targeted LDP sessions because the NFM-P provides targeted-LDP management.

Checkpoints are not supported on MPLS.

5.2 Workflow for MPLS topology map management

5.2.1 Stages

1. Open an MPLS topology map.
2. View the relationship between objects drawn on the map.
3. Identify missing MPLS/RSVP links.
4. Identify missing LDP links.

5.3 To identify missing MPLS/RSVP links

5.3.1 Steps

1

Choose Tools→Route Analysis→MPLS Topology→*IGP_Administrative_Domain* from the NFM-P main menu.

The MPLS topology map appears showing the network objects.

2

Right-click on the map area and choose MPLS/RSVP Links→Missing Links→Find Missing MPLS/RSVP Links from the MPLS topology view contextual menu. The List Missing MPLS/RSVP Links dialog box opens. To list non-managed missing links, click on the Yes button. Otherwise, click on the No button. The missing links are highlighted on the map.

3

Close the MPLS topology map.

END OF STEPS

5.4 To identify missing LDP links

5.4.1 Steps

1

Choose Tools→Route Analysis→MPLS Topology→*IGP_Administrative_Domain* from the NFM-P main menu.

The MPLS topology map appears showing the network objects.

2

Right-click on the map area and choose LDP Links→Missing Links→Find Missing LDP Links from the MPLS topology view contextual menu. The List Missing LDP Links dialog box opens. To list non-managed missing links, click on the Yes button. Otherwise, click on the No button. The missing links are highlighted on the map.

3

Close the MPLS topology map.

END OF STEPS

5.5 To highlight IGP links

5.5.1 Steps

1

Choose Tools→Route Analysis→MPLS Topology→*IGP_Administrative_Domain* from the NFM-P main menu.

The MPLS topology map appears showing the network objects.

2

Right-click on the map area and choose Highlight IGP Links from the MPLS topology view contextual menu. The Select IGP Filter form opens.

3

Specify a filter to search for IGP links and click on the OK button. The IGP links are highlighted on the topology map.

4

To remove the IGP link highlights, right-click on the map area and choose Clear:Highlight IGP Links from the contextual menu.

5

Close the MPLS topology map.

END OF STEPS

6 Topology references

6.1 Topology references overview

6.1.1 Introduction to topology references

A reference determines the operational state of the real network, specifically for subnets and links.

The CPAM automatically sets a reference on all of the topology objects when an object is created or after a software upgrade. If topology objects exist from previous software versions, the topology objects are automatically referenced.

6.1.2 References on the topology maps

A topology reference is used to determine and track the existence of an object. Topology maps on the GUI are highlighted with colors to indicate the status of a link.

The following colors identify the links on the IGP and MPLS topology maps:

- green for operationally up links that are added after a reference time
- light green for referenced links that are operationally up
- red for referenced links that are operationally down or have been removed (the adjacency between two router is removed)
- white for groups that contain links with different colors. For example, a green and grey link. If there is a red link, the entire group is red.

The following color conventions are used on OSPF topology maps:

- link colors are based on area, whether or not they are in the reference
- red links are referenced links that are operationally down
- white links are link groups that contain links from multiple areas. A red link makes the entire group red.

The following color conventions are used on ISIS topology maps:

- link colors are based on level, whether or not they are in the reference
- red links are referenced links that are operationally down
- white links are link groups that contain links from multiple levels. A red link makes the entire group red.

The NFM-P database continues to store information for the reference link after it has been removed from the LSDB. Although the link is displayed in red, the original color of the link reappears after the link is rediscovered by the CPAA. The state of the router is not indicated by a color.

6.1.3 Topology reference functions

The following table describes the CPAM reference functions:

Table 6-1 CPAM reference functions

Function	Description
Cleanup Reference→All ISIS Domains	References are maintained for all of the links, routers, and areas that are operationally up within ISIS routing domains in an IGP administrative domain. All operationally down objects are removed from the topology map.
Cleanup Reference→All OSPF Areas	References are maintained for all of the links, routers, and areas that are operationally up within OSPF areas in an IGP administrative domain. All operationally down objects are removed from the topology map.
Cleanup Reference→All	References are maintained for all of the links, routers, and areas that are operationally up in all of the ISIS routing domains and OSPF areas in an IGP administrative domain. All operationally down objects are removed from the topology map.

6.2 Workflow for topology references

6.2.1 Stages

1

View topology map and link colors.

2

Manage topology references:

- clean up references

6.3 To manage topology references in an IGP administrative domain

6.3.1 Steps

1

Choose Tools→Route Analysis→Checkpoints from the NFM-P main menu. The Checkpoint Manager form opens.

2

Choose IGP Administrative Domain (CPAM: Topology) from the object drop-down menu.

3

Specify a filter for the search, if required, and click on the Search button. A list of IGP administrative domains appears.

4

Choose an entry and click on the Properties button. The IGP Administrative Domain (Edit) form appears with the General tab displayed.

5

Click on the Cleanup button and choose one of the following:

- ISIS Reference
- Non-Routed Reference
- OSPF Reference
- All References

If the Cleanup button is not visible, click on the More Actions button and choose Cleanup. A dialog box appears.

See Table 6-1, “CPAM reference functions” (p. 82) for a description of each function.

6

Click on the Yes button.

7

Close the IGP Administrative Domain (Edit) form.

8

Close the Checkpoint Manager form.

END OF STEPS

7 Map highlighting

7.1 Map highlighting overview

7.1.1 Introduction to map highlighting

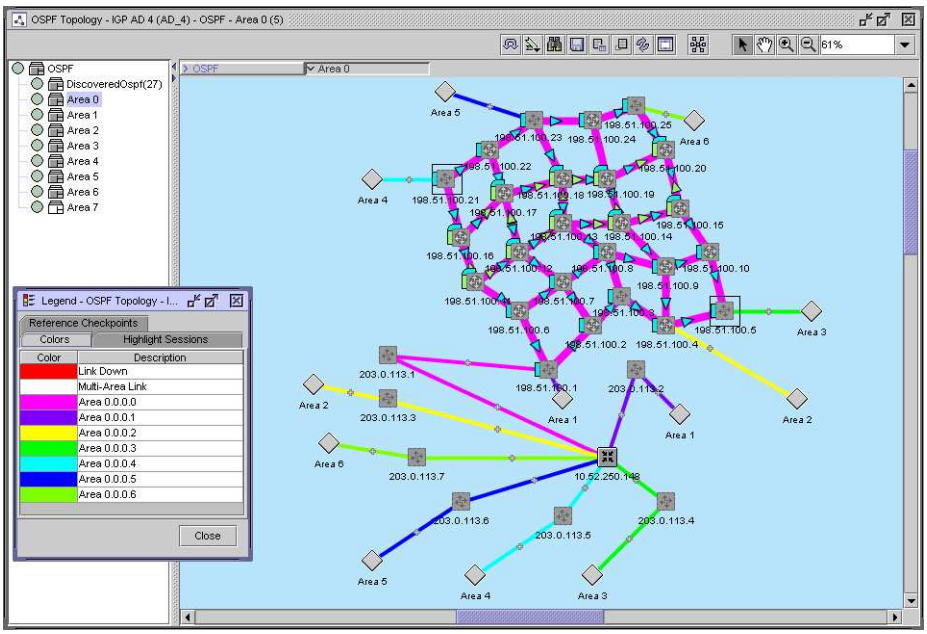
The CPAM allows you to highlight L2/L3 services, composite services, service tunnels, SPF and CSPF calculations, multicast trees, and OAM diagnostics results on IGP maps.

The CPAM supports the highlighting of up to six objects on a link or link group. You can draw multiple objects over a map by adding an arrow icon on top of the link used by the object. The links that are used by the highlighted objects become thicker to increase path visibility. Highlighted routers use a colored section on the router icon. The router or group icon supports the display of up to six colored sections.

The highlighted objects do not have to be a persistent object—for example, the calculated route between two routers is a transient object. In addition, the highlighted objects do not have to be of the same type—for example, you can highlight an LSP actual path and the shortest path between two routers on the same L3 topology map.

The SPF calculation results in the application of the same color for all of the highlighted links used by an ECMP route. For example, if the shortest paths between R1 and R4 are (one path) R1, R2, R3, R4, and (another path) R1, R2, R3, R4, then links R1-R2 (common link), R2-R3, R3-R4, R2-R3, R3-R4, are highlighted by one color. The following figure shows an OSPF topology map with SPF calculation results for links used by an ECMP route.

Figure 7-1 SPF calculation highlight



When a link in a link group is highlighted, the link group is highlighted as well.

7.1.2 CPAM on-demand SPF calculation

The CPAM can highlight the shortest path from a source IP address to a destination IP address. The source or destination can be any IPv4 address, or on ISIS and OSPFv3 topology maps, an IPv6 address. See 7.6 “To highlight the shortest path between two IP addresses” (p. 97).

The CPAM does not establish a route if the CPAAs cannot resolve one or more of the IP addresses. The CPAM supports intra- and inter-area IP routes.

The IP subnets outside of the OSPF routing areas can be learned by BGP, for example. If the BGP subnets are redistributed to the OSPF protocol by the ASBR router as external routes, the CPAA can determine the shortest path between two subnets.

The route calculation process evaluates ECMP and displays equal cost routes on the topology map.

It is possible for the actual route provided by the network to differ from the calculated route because of unexpected router configurations on the route. The CPAA and the CPAM do not assess the route policies and ACL filters configured on the routers.

Note: SPF calculations on OSPF topology maps consider only the route in OSPF.
SPF calculations on OSPFv3 topology maps consider only the route in OSPFv3.
SPF calculations on ISIS topology maps consider only the route in ISIS.
SPF calculations on IGP topology maps are multi-protocol.

7.1.3 SPF calculation with IGP shortcut

If you configure an LSP as an IGP shortcut, all of the destinations along the IGP SPF path that are downstream of the shortcut termination use the shortcut as a means to reach those destinations.

Note: IGP shortcuts are configurable only through XML API.

If OSPF is used as the IGP, the LSPs that are configured as IGP shortcuts are sent to the OSPF routing protocol and are used in its SPF calculation to determine the destinations that should use the LSPs.

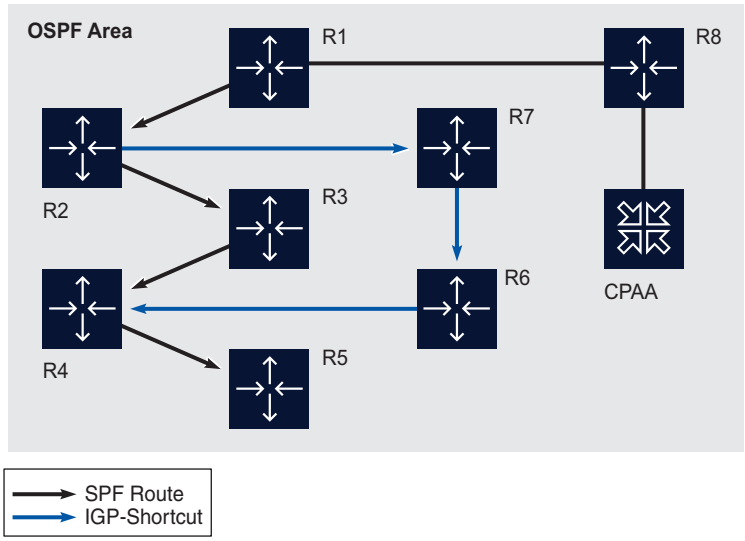
When an LSP IGP shortcut is configured on a node, the shortcut remains local to that node and is not flooded to the other nodes in the network. As a result, the CPAA does not know that IGP shortcuts exist unless this information is provided to it through a CPAM XML API.

Sample configurations

The following sample configurations describe how the CPAM uses the IGP shortcut in the SPF calculation.

The sample network displayed in the figure below has 8 routers (R1 to R8) and one CPAA. An IGP shortcut is configured between R2 and R4. R2 supports the IGP shortcut.

Figure 7-2 Sample OSPF network with IGP shortcut



As a first example, the CPAA receives a shortest path request from R1 to R5. If the IGP shortcut were not configured, the calculated SPF route would be the following:

R1→R2→R3→R4→R5

Because an IGP shortcut is configured between two endpoints of the calculated SPF route, the CPAA returns the following SPF route:

R1→R2→IGP_shortcut→R4→R5

In a second example, the CPAA receives a shortest path request from R1 to R3. If the IGP shortcut were not configured, the calculated SPF route would be the following:

R1→R2→R3

In this case, the CPAA does not use the IGP shortcut because the R4 endpoint of the LSP is not included in the calculated shortest path. As a result, the CPAA returns the same SPF route:

R1→R2→R3

7.1.4 On-demand SPF and BGP prefixes

Within the CPAM, on-demand SPF applies only to IGP routes. If a prefix is not visible in the IGP domain the on-demand SPF fails. The CPAM supports BGP prefixes in one AS—prefixes learned through IBGP. The path is highlighted up to the router that advertises the prefix into the AS. This is the originating router for internal routes and exit router for external routes.

If you run SPF on an OSPF, ISIS, or IGP topology map, the CPAM verifies whether the destination prefix is known to IGP. source address should be a routerId or interface IP address known to IGP. If the destination is an internal or external IGP address, the CPAM performs the SPF calculation

If the destination address is not an IGP address, the CPAM looks into BGP routes. If the destination is reachable through a BGP route, the CPAM determines the best next hop for the BGP route by running the BGP route selection criteria, and then highlights the shortest path to the next hop. The highlight session identifies whether the destination is a BGP or IGP route.

Note: For BGP confederations, if multiple IGP administrative domains are used, the path is highlighted only up to the edge of the IGP domain.

For BGP confederations, if the source router is a managed router, the CPAM finds the sub-AS for the source router and sends the request to the CPAA that manages the sub-AS. If the source router is not managed, requests are sent to one of the CPAAs in the confederation. If the CPAA is located in another sub-AS from the source router, only one next hop is visible for the destination, which may not be the best one from the source router.

If there are multiple BGP ASes under one IGP administrative domain, the path to the BGP route is highlighted only if the source router is managed.

7.1.5 Next hop highlights

The CPAM supports next hop highlighting in a routing path. You can use next hop highlighting to view the reachability to an IP address from a set of source routers. For example, if the IP address for which you want to view reachability VoD server at a location and that VoD server cannot be reached from some parts of the network, you can use the next hop highlighting tool to view the routers that can see the VoD server.

The next hop shows which egress interface or link is used from the source router to reach the FEC.

See Chapter 14, “Root cause analysis” for information about how to configure next hop highlighting.

7.1.6 Historical SPF highlights

The CPAM supports the highlighting of historical IP path records. See Chapter 14, “Root cause analysis” for information about historical SPF highlighting.

7.1.7 CSPF highlights

CSPF is an extension to the SPF algorithm that calculates the shortest path based on a set of constraints. The links on the topology map that do not meet the set of constraints are removed before the CPAM performs the SPF calculation.

Consider the following when you configure CSPF highlighting:

- CSPF is calculated only within one OSPF area. The source and destination must exist in the same area. The source must be a router or an interface. The destination can be any valid IP address within the area.
- CSPF is cannot be calculated from L1 to L2. CSPF cannot be calculated within an L1 of different instances.
- CSPF cannot be calculated across IGP boundaries or ASs.
- The CPAM does not validate whether the source and destination routers are in the same area. If the routers are in different areas, the CSPF operation fails.

SRLG support

A set of links can be considered a shared risk link group if they share a resource whose failure may affect all of the links in the set. A link can belong to multiple SRLGs. An SRLG is identified by a 32-bit number that is unique within an IGP domain.

The CPAM can use an SRLG list as a constraint for the CSPF calculation. You can add all of the SRLG values that must be excluded in the CSPF calculation.

7.1.8 OAM diagnostics results highlights

The CPAM supports the highlighting of the following OAM diagnostics results:

- Multicast trace
- LSP trace
- ICMP route trace

See Chapter 13, “OAM diagnostics” for information about OAM diagnostics highlighting.

7.1.9 BGP highlights

You can use the CPAM to highlight all of the NEs that advertise a prefix into an AS on the IGP topology map. You must specify a BGP prefix, and an RD for VPN IPv4 prefixes. The CPAM highlights all of the NEs that advertise a route for that prefix into the administrative domain. The preferred exit router or routers, based on the BGP attributes, are highlighted in another color from the other exit routers.

See Chapter 10, “BGP management” for information about how to configure BGP highlighting.

7.2 Tunnel and service topology highlights

7.2.1 Service tunnel highlights

You can highlight a service tunnel on the OSPF, ISIS, and IGP topology views. The tunnel type determines the method that is used by the CPAM to identify the path.

- A GRE tunnel path is derived from the SPF calculation between the source and destination routers.
- The path of an LDP tunnel is the result of an OAM LSP trace diagnostic (the destination has a /32 prefix). The source router must be capable of handling the LSP OAM diagnostic.

See 7.20 “To highlight service tunnels” (p. 110).

7.2.2 Service highlights

The highlighting of services is an extension of tunnel highlighting. All PE routers and service tunnels used by the service are highlighted on the OSPF, ISIS, and IGP topology views. Although you can select and highlight one or more SDP bindings in a service, Nokia recommends that you use limited highlighting for services with multiple PE routers. You can highlight services with active SDP bindings, or both active and standby. You can also highlight the actual path that packets from an EPIPE service with an LDP tunnel are taking within the network. Furthermore, you can use the CPAM to highlight composite services and services between edge devices and aggregator devices.

See 7.21 “To highlight services” (p. 111) , 7.22 “To highlight composite services” (p. 112), and

7.23 “To highlight services from the topology map” (p. 113).

7.2.3 Seamless MPLS highlights

Seamless MPLS uses LDP or RSVP and BGP to create services that span multiple IGP domains or areas. This is accomplished by providing a transport tunnel that can be used by service tunnels in different IGP domains or areas to carry traffic, effectively stitching them together. When highlighting a service or service tunnel, the transport tunnel that allows for seamless MPLS will appear as a dashed line.

7.2.4 VPRN prefix path highlighting

You can highlight the path for a VPRN prefix by selecting a source site in the VPRN and configuring the highlight. In addition to specifying the IP address and prefix length, you must choose the administrative domain and the type of map—IGP, OSPF, or ISIS. The route path is highlighted on the specified map, or an error message is displayed if the path is not found.

To find the path, the CPAM verifies the VPRN routing table. In addition, an SNMP community string should be configured for the VPRN site. If a prefix of the protocol type BGP VPN does not exist in the VPRN routing table, an error message is displayed.

If the CPAM finds an entry in the VPRN routing table, the next hop for the prefix is also returned. If the VPRN is using GRE or LDP, the path is highlighted using SPF from the source site to the route next hop.

Note: You must ensure that the community string is configured on the VPRN site in order to highlight the VPRN prefix path. Otherwise, the CPAM uses the base routing table and not the service routing table to calculate the highlight, and returns the wrong result.

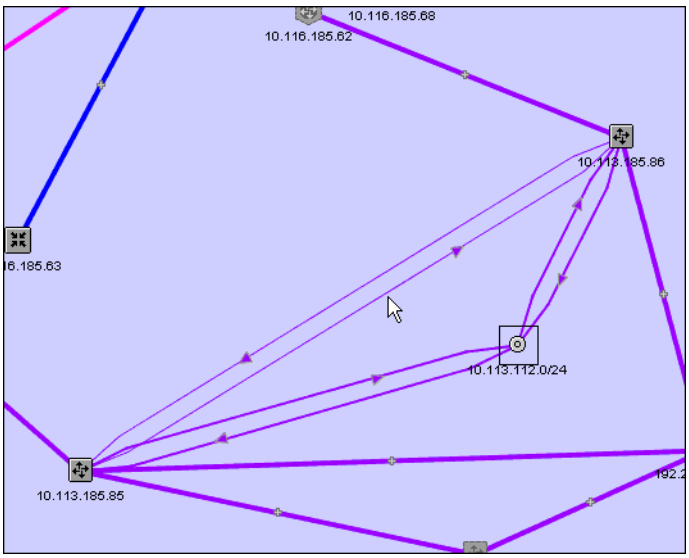
VPRN prefix path highlighting is supported on a 7450 ESS or 7750 SR.

See 7.24 “To highlight a VPRN prefix path” (p. 114).

7.2.5 IES IGP link highlighting

You can use the CPAM to highlight IGP links of IES services on a topology map. For example, when two IES services with OSPF interfaces are connected through spoke SDP bindings between the two adjacent routers using RSVP-TE LSP, the primary path uses the direct link between the two routers. The standby path follows a strict route around the ring in the opposite direction. When the direct link between the two routers fails, the actual traffic goes through the standby LSP path. The OSPF links between the IES services remain operational and the PIM topology is not affected. An IES IGP link is a logical link and is displayed on the map as a thin line, as displayed in the following figure:

Figure 7-3 IES OSPF interface



See 7.25 “To highlight IES IGP links” (p. 115).

7.3 Dynamic RSVP LSP highlights

7.3.1 General information

An LSP can have one provisioned primary path and multiple standby and secondary paths. Both the primary and standby paths can be operationally up at the same time. Traffic flows only on the active path. The CPAM allows you to highlight the following LSP paths:

- active path
- operational path or paths (primary and standby paths)
- the provisioned path of the active path

  Note:

  The actual path may not always follow the provisioned path. For example, if fast reroute has occurred, the actual path uses one or more bypass tunnels.
- provisioned paths (primary, secondary, and standby LSP paths)
- historical paths

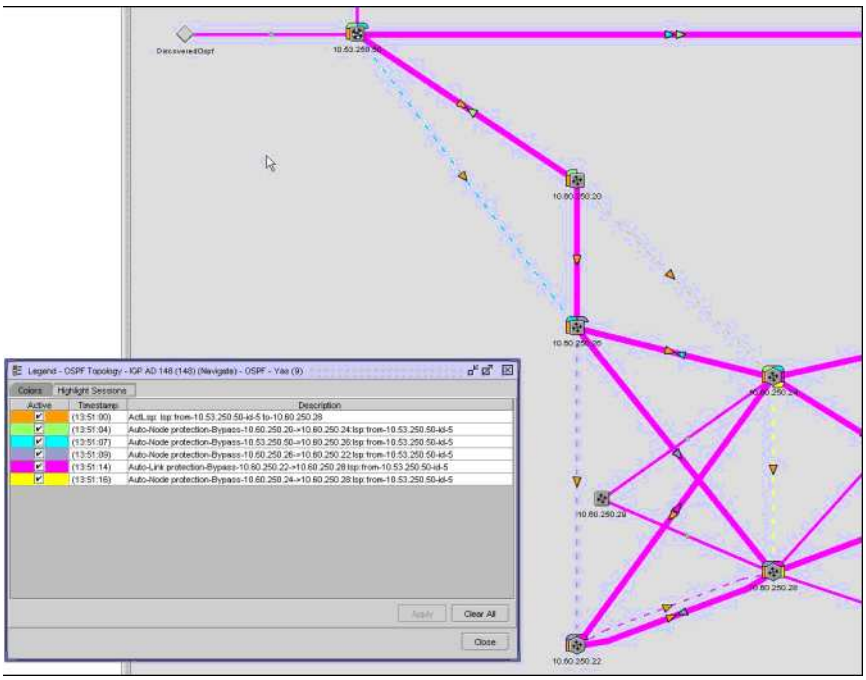
7.3.2 Bypass tunnel highlighting for LSP paths

The CPAM monitors the active path of an LSP. The monitored path can include bypass tunnels when FRR is configured. The CPAM highlights all of the available auto and manual bypass tunnels when the associated LSP path is highlighted. The bypass tunnel is highlighted in the same color as the LSP path, with a dotted line. In addition, if an unused bypass tunnel exists between two NEs, a

dotted line is displayed. You can highlight the actual path of the bypass tunnel by right-clicking on the tunnel and selecting the contextual menu option. Bypass tunnel highlighting is supported only on NFM-P-managed NEs.

The figure below shows an FRR LSP path with bypass tunnel auto-link and auto-node protection between NFM-P-managed NEs. The dotted line is a logical path that represents the bypass tunnel that is used.

Figure 7-4 Bypass tunnel Hightlight



Bypass tunnel highlighting allows you to quickly determine how an LSP path is protected by FRR, whether FRR is active in any part of the path, and where it is active.

7.3.3 GNE support

The CPAM supports the limited management of GNEs. The CPAM support of GNEs requires the proper MIB support on GNEs.

Note: Standard MIBs support read-only mode for the path objects. LSPs or paths can not be configured from the NFM-P.

The NFM-P mediation engine supports standard MPLS MIBs. The GNEs managed by the NFM-P using standard MIBs must use attributes, IDs and traps in a specific manner to ensure proper operation. Otherwise, LSP objects may be represented incorrectly in the NFM-P.

See Appendix Appendix A, “CPAM MIB support for GNEs” for information about MIB support. See “To prepare a GNE for NFM-P management” in the *NSP NFM-P Classic Management User Guide* for information about how to add a routing MIB to a GNE profile.

7.4 Audit of highlighted paths

7.4.1 General information

The CPAM highlighted path audit verifies each interface that is highlighted in a path. The CPAM compares each audit calculation to a threshold that you configure. The audit threshold verification includes:

- Ethernet and POS interface utilization and error rates
- IP interface utilization and error rates
- SROS queue utilization and errors

The audit uses a count that is based on the difference between the capture of two real-time statistics that are separated by a configurable time delay.

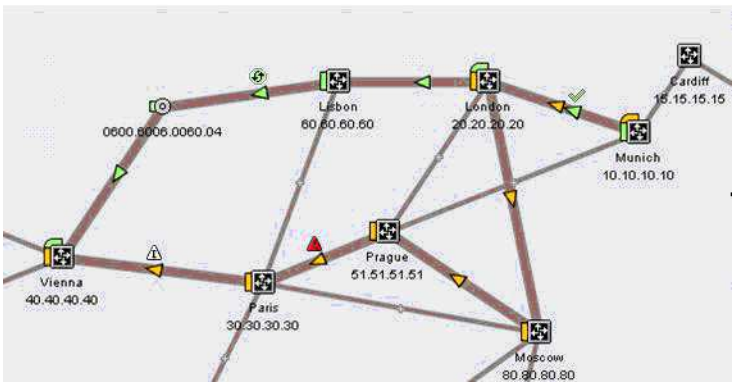
When you start an audit, the following status icons appear next to the audited links on the topology map:

- In Progress
- Failed
- Succeeded
- Indeterminate
- Not applicable (no icon)

  Note:

  Links with a not applicable status (no icon) are typically a graphical representation of a more complex connection, and audit results may be represented in an adjacent link.

Figure 7-5 Audited highlighted paths



On the Browse Statistics form, the following MIBs are used in highlighted path audit:

- Ethernet Stats (Ethernet Equipment)
- Interface Stats (Physical Equipment)
- Port Net Egress Accounting Stats (Physical Equipment)

- Port Net Ingress Accounting Stats (Physical Equipment)
- SONET Line Current Stats (SONET Equipment)
- SONET Section Current Stats (SONET Equipment)

Note: tmnxMcPathOperChlTable, used for FC fabric resource audit, is not visible in the NFM-P client.

See 4.22 “To view the legends for a topology map” (p. 71) for information about how to view the icon legend. See 7.31 “To perform a highlighted path audit” (p. 121) for information about how to configure the audit.

7.5 Workflow for map highlighting

7.5.1 Stages

1

Determine the map type you want to view:

- maps that show IGP topology
- maps that show protocol-specific topologies

2

View the relationship between objects drawn on the map.

3

Highlight the shortest path between two IP addresses. See 7.6 “To highlight the shortest path between two IP addresses” (p. 97) for more information.

4

Highlight the bidirectional shortest path between two IP addresses. See 7.7 “To highlight the bidirectional shortest path between two IP addresses” (p. 98) for more information.

5

Highlight the shortest path between two IP addresses and highlight the LFA path. See 7.8 “To highlight the shortest path between two IP addresses and highlight LFA path” (p. 99) for more information.

6

Highlight the LFA path. See 7.9 “To highlight the LFA path” (p. 99) for more information.

7

Highlight the shortest path between two IP addresses, run a ping, and highlight ping test results. See 7.10 “To highlight the shortest path between two IP addresses, run a ping, and highlight ping test results” (p. 100) for more information.

8

Highlight the path for the default route from a source. See 7.12 “To highlight the path for the default route from a source” (p. 104) for more information.

9

Highlight PTP clock paths. See 7.15 “To highlight PTP Clock paths” (p. 106) for more information.

10

Highlight PTP status. See 7.16 “To highlight PTP status” (p. 107) for more information.

11

Create a Source Entry Point between managed PTP peers to an unmanaged PTP peer. See 7.17 “To create a Source Entry Point between Managed PTP Peers to an unmanaged PTP Peer” (p. 108) for more information.

12

Highlight PTP peers in a Sync Domain. See 7.18 “To highlight PTP Peers in a Sync Domain” (p. 109) for more information.

13

Highlight the constrained shortest path between two IP addresses. See 7.11 “To highlight the constrained shortest path between two IP addresses” (p. 101) for more information.

14

Diagnose a CSPF failure by highlighting the links within the specified routing domain that meet or do not meet the specified constraints. See 7.14 “To diagnose a CSPF failure” (p. 106) for more information.

15

Highlight the network route between two routers. See 7.13 “To highlight the network route between two routers” (p. 105) for more information.

16

Highlight service tunnels. See 7.20 “To highlight service tunnels” (p. 110) and 7.23 “To highlight services from the topology map” (p. 113) for more information.

17

Highlight services. See 7.23 “To highlight services from the topology map” (p. 113) and 7.21 “To highlight services” (p. 111) for more information.

18

Highlight composite services. See 7.22 “To highlight composite services” (p. 112) for more information.

19

Highlight a VPRN prefix path. See 7.24 “To highlight a VPRN prefix path” (p. 114) for more information.

20

Highlight IES IGP links. See 7.25 “To highlight IES IGP links” (p. 115) for more information.

21

Highlight historical IP paths. See 7.26 “To highlight historical IP paths” (p. 116) for more information.

22

Highlight LSP paths. See 7.27 “To highlight LSP paths” (p. 117) for more information.

23

Highlight S2L LSP paths. See 7.28 “To highlight S2L LSP paths” (p. 118) for more information.

24

Highlight point-to-multipoint LSPs. See 7.29 “To highlight point-to-multipoint LSPs” (p. 120) and 7.30 “To highlight point-to-multipoint LSPs from the topology map contextual menu” (p. 121) for more information.

25

Audit highlighted paths, if required. See 7.31 “To perform a highlighted path audit” (p. 121) for more information.

26

Manage active highlights, as required. See 7.32 “To manage active highlights on a topology map” (p. 123) for more information.

27

View highlights on a flat map. See 7.33 “To view highlights on a flat map” (p. 123) for more information.

28

Manage info tables.

- Create an info table configuration for map objects. See 7.34 “To use the Configure Info Tables button” (p. 124) for more information.
- Display configured info tables on the map view. See 7.35 “To use the Global Info Tables button” (p. 125) for more information.
- Apply an info table configuration to a map object or highlight. See 7.36 “To apply an info table

configuration to a map object" (p. 97) and 7.37 "To apply an info table configuration to a map highlight" (p. 126) for more information.

7.6 To highlight the shortest path between two IP addresses

7.6.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate IGP topology map opens.

2

Perform one of the following:

a. Right-click on the map and choose Highlight→Paths→IP→SPF from the contextual menu. The Find Object form opens. Continue to Step 3 .

b. Right-click on a router and choose Highlight SPF from the contextual menu. The Find Object form opens with the value of the First IP parameter populated. Go to Step 4 .

3

Configure the First IP parameter or use the Select button to select a router if the source IP address is a router.

4

Configure the Second IP parameter or use the Select button to select a router if the destination IP address is a router.

Note: Alternatively, you can press the Ctrl key and click on a source and destination router or link, right-click and choose Highlight SPF from the contextual menu. The First IP and Second IP parameters are configured with the IP address of the selected routers.

5

Click on the OK button. The Find Object form closes and the SPF is highlighted on the topology map.

6

To remove the SPF highlight, perform 7.32 "To manage active highlights on a topology map" (p. 123) .

END OF STEPS

7.7 To highlight the bidirectional shortest path between two IP addresses

7.7.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate IGP topology map opens.

Note: The highlighting of bidirectional shortest paths between two IP addresses is not supported on OSPFv3 topology maps.

2

Perform one of the following:

a. Right-click on the map and choose Highlight→Paths→IP→SPF from the contextual menu. The Find Object form opens. Continue to Step 3 .

b. Right-click on a router and choose Highlight SPF from the contextual menu. The Find Object form opens with the value of the First IP parameter populated. Go to Step 4 .

3

Configure the First IP parameter or use the Select button to select a router if the source IP address is a router.

4

Configure the Second IP parameter or use the Select button to select a router if the destination IP address is a router.

Note: Alternatively, you can press the Ctrl key and click on a source and destination router or link, right-click and choose Highlight Bidirectional SPF from the contextual menu. The First IP and Second IP parameters are configured with the IP address of the selected routers.

5

Click on the OK button. The Find Object form closes and the bidirectional SPF is highlighted on the topology map.

6

To remove the bidirectional SPF highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

END OF STEPS

7.8 To highlight the shortest path between two IP addresses and highlight LFA path

7.8.1 General information

A Loop-Free Alternate (LFA) path is pre-computed by the node as a backup next-hop for forwarding in-transit and CPM-generated IP packets when the primary next-hop is not available. This path enables the node to resume forwarding IP packets to a destination prefix without waiting for the routing convergence. SPF with LFA highlights can be performed on OSPF,OSPFv3, and ISIS topology maps.

7.8.2 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate IGP topology map opens.

2

Perform one of the following:

a. Specify the source and destination IP addresses on the Find Object form.
   1. Right-click on the map and choose Highlight→Paths→IP→SPF with LFA from the contextual menu. The Find Object form opens.
   2. Configure the First IP parameter and the Second IP parameter, or click Select to select routers.
   3. Click OK. The shortest path and the LFA path are highlighted.

b. Specify the source and destination IP addresses on the topology map.
   1. Press the Ctrl key and click on a source and a destination router or link.
   2. Right-click and choose Highlight SPF with LFA. The shortest path and the LFA path are highlighted.

3

To remove the SPF with LFA highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

End of steps

7.9 To highlight the LFA path

7.9.1 General information

SPF with LFA highlights can be performed on OSPF,OSPFv3, and ISIS topology maps.

7.9.2 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate IGP topology map opens.

2

Perform one of the following:

a. Specify the source and destination IP addresses on the Find Object form.
   1. Right-click on the map and choose Highlight→Paths→IP→LFA from the contextual menu. The Find Object form opens.
   2. Configure the First IP parameter and the Second IP parameter, or click Select to select routers.
   3. Click OK. The LFA path is highlighted.

b. Specify the source and destination IP addresses on the topology map.
   1. Press the Ctrl key and click on a source and a destination router or link.
   2. Right-click and choose Highlight LFA. The LFA path is highlighted.

3

To remove the LFA highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

END OF STEPS

7.10 To highlight the shortest path between two IP addresses, run a ping, and highlight ping test results

7.10.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate IGP topology map opens.

2

Right-click on the map and choose Highlight→Paths→IP→SPF with Ping from the contextual menu. The Find Object form opens.

3

Configure the First IP parameter or use the Select button to select a router if the source IP address is a router.

4

Configure the Second IP parameter or use the Select button to select a router if the destination IP address is a router.

Note: Alternatively, you can press the Ctrl key and click on a source and destination router or link, right-click and choose Highlight SPF from the contextual menu. The First IP and Second IP parameters are configured with the IP address of the selected routers.

5

Click on the OK button. The Find Object form closes and the SPF and ping test results are highlighted on the topology map.

6

To remove the SPF and ping test results highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

END OF STEPS

7.11 To highlight the constrained shortest path between two IP addresses

7.11.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate IGP topology map opens.

2

Perform one of the following:

a. Right-click on the map and choose Highlight→Paths→IP→CSPF from the contextual menu. The Highlight CSPF Request form opens with the General tab displayed.

b. Perform the following:

1. Press the Ctrl key and click on a source and destination router or link.
2. Right-click on the map and choose Highlight→Paths→IP→CSPF from the contextual menu. The Highlight CSPF Request form opens with the General tab displayed.

3

Configure the parameters:

- Protocol
- Request Type
- Least Fill Min Threshold %
- Required Bandwidth

- Hop Limit
- SRLG Strict

The Least Fill Min Threshold % parameter is configurable only when the Request Type parameter is set to Least_Fill.

4

Perform one of the following:

a. Configure the Source IP parameter.

Note: If you performed Step 2 b , the Source IP parameter is already configured with the selected source router or link IP address.

b. Choose a source link or router.

1. Click on the Select button. The Select Source Router form opens.
2. Choose a source type from the menu:
   - *Protocol* Link (CPAM: Topology) to search for a link
   - Router (CPAM: Topology) to search for a router
3. Specify a filter, if necessary, and click on the Search button. A list of routers or links appears.
4. Choose an entry and click on the OK button. The Select Source Router form closes and the Highlight CSPF Request form reappears with the source information.

5

Perform one of the following:

a. Configure the Destination FEC parameter.

Note: If you performed Step 2 b , the Destination FEC parameter is already configured with the destination router or link IP address.

b. Choose a destination.

1. Click on the Select button. The Select Destination FEC form opens.
2. Choose a destination type from the menu:
   - *Protocol* Link (CPAM: Topology) to search for links
   - Router (CPAM: Topology) to search for a routers
3. Specify a filter, if necessary, and click on the Search button. A list of routers or links appears.
4. Choose an entry and click on the OK button. The Select Destination FEC form closes and the Highlight CSPF Request form reappears with the destination information.

6

Click on the Administrative Groups tab.

7

Choose an administrative group from the Unassigned list in the Included Groups panel and click on the right arrow button. The administrative group moves to the Assigned list.

Note: The links in the calculated CSPF must include the specified administrative groups.

8

Choose an administrative group from the Unassigned list in the Excluded Groups panel and click on the right arrow button. The administrative group moves to the Assigned list.

Note: The links in the calculated CSPF must exclude the specified administrative groups.

9

Specify the routers that are to be excluded from the CSPF highlight. The highlighted CSPF must not pass through the routers with the specified router IDs.

1. Click on the Excluded Routers tab.
2. Click on the Add button. The Select Excluded Routers form opens.
3. Specify a filter, if necessary, and click on the Search button. A list of routers appears.
4. Choose one or more routers and click on the OK button. The Select Excluded Routers form closes.

10

Specify the egress IP addresses that are to be excluded from the CSPF highlight. The highlighted CSPF must not pass through the egress interfaces with the specified IP addresses.

1. Click on the Excluded Egress IP Addresses tab.
2. Click on the Add button. The Select Excluded Egress IP Links form opens.
3. Click on the Select Object Type button and choose one of the following:
   - ISIS Link (CPAM:Topology)
   - Non-Routed Link (CPAM: Topology)
   - OSPF Link (CPAM:Topology)
4. Specify a filter and click on the Search button.
5. Choose one or more links and click on the OK button. The Select Excluded Egress IP Links form closes.

11

Configure the TE parameters, if required.

1. Click on the TE Parameters tab.
2. Configure the parameters:
   - System Instance ID
   - Diff-Serv Class Type
   - Setup Priority
   - Hold Priority

12

Specify the values of SRLG to be excluded from the CSPF calculation by choosing specific values or choosing links from which SRLG values are to be excluded:

1. Click on the Excluded Shared Risk Link Groups tab.
2. Click on the Add Links button. The Select IP Link with excluded SRLG form opens.
3. Click on the Search button. A list of links appears.
4. Choose a link and click on the OK button. The Select IP Link with excluded SRLG form closes.
5. To add more links, repeat 2 to 4 .
6. Click on the Add Values button. The Add excluded SRLG Value form opens.
7. Configure the SRLG Value parameter.
8. Click on the OK button. The Add excluded SRLG Value form closes.
9. To add more values, repeat 6 to 8 .

13

Click on the OK button. The Highlight CSPF Request form closes and the CSPF is highlighted on the topology map.

Note: If the CSPF requests fails and the Diagnose CSPF Failure window appears, see 7.14 “To diagnose a CSPF failure” (p. 106) .

14

To manage or remove the CSPF highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

END OF STEPS

7.12 To highlight the path for the default route from a source

7.12.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate IGP topology map opens.

2

Perform one of the following:

a. Right-click on the map and choose Highlight→Paths→IP→SPF from the contextual menu. The Find Object form opens. Continue to Step 3 .

b. Right-click on a router and choose Highlight SPF from the contextual menu. The Find Object form opens with the value of the First IP parameter populated. Go to Step 4 .

3

Configure the First IP parameter or use the Select button to select a router if the source IP address is a router.

4

Configure the Second IP parameter to a value of 0.0.0.0/0.

5

Click on the OK button. The Find Object form closes and the default route is highlighted on the topology map.

6

To remove the default route highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

END OF STEPS

7.13 To highlight the network route between two routers

7.13.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate topology map appears showing the network objects.

2

Click on the source router.

3

Press the Ctrl key and click on the destination router.

4

Right-click on the map and choose Highlight→Paths→IP→SPF from the contextual menu. The SPF is highlighted on the map.

5

To manage or remove the SPF highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

END OF STEPS

7.14 To diagnose a CSPF failure

7.14.1 General information

When a CSPF highlight request fails, perform this procedure to highlight the links within the specified routing domain that meet or do not meet the specified constraints.

Note: A message is displayed in the Diagnose CSPF Failure window if the source or destination IP address is invalid.

7.14.2 Steps

1

Run the CSPF highlight request by performing 7.11 “To highlight the constrained shortest path between two IP addresses” (p. 101) . The Diagnose CSPF Failure window appears if the configuration is invalid.

2

Perform one or more of the following:

a. Click on the Retry button to close the Diagnose CSPF Failure window and reopen the Highlight CSPF Request form. Configure the parameters, as described in 7.11 “To highlight the constrained shortest path between two IP addresses” (p. 101) .

b. Click on the Details button to open a read-only copy of the Highlight CSPF Request form and view the configured parameters.

c. Click on the Qualified Links button to highlight the links in the routing domain that meet the configured constraints. This button is enabled only when the routing domain is known, that is, the source and destination IP addresses are valid.

d. Click on the Unqualified Links button to highlight the links in the routing domain that do not fulfill the configured constraints. This button is enabled only when the routing domain is known, that is, the source and destination IP addresses are valid.

3

Click on the OK button to close the Diagnose CSPF Failure window.

END OF STEPS

7.15 To highlight PTP Clock paths

7.15.1 General information

This procedure only applies to IEEE 1588 PTP Synchronization-enabled NEs.

7.15.2 Steps

1

Choose Tools→Route Analysis→IGP Topology from the NFM-P main menu. The IGP topology map opens.

2

Perform one of the following:

a. Right-click on the map and choose Highlight→Synchronization→PTP Clock Upstream from the contextual menu. The Select PTP Clock form opens.

b. Right-click on the map and choose Highlight→Synchronization→PTP Clock Downstream from the contextual menu. The Select PTP Clock form opens.

3

Click on the Search button. A list of PTP Clock entries is displayed.

4

Select a PTP Clock entry from the list and click the OK button.

The Select PTP Clock form closes. The dotted line and arrow indicate the direciton of the clock and peer-to-peer connection. An information message is also displayed.

5

To remove the path highlights, refer to 7.32 “To manage active highlights on a topology map” (p. 123) .

END OF STEPS

7.16 To highlight PTP status

7.16.1 Steps

1

Choose Tools→Route Analysis→IGP Topology from the NFM-P main menu. The IGP topology map opens.

2

Perform one of the following:

a. Right-click on the map and choose Highlight→Synchronization→Domain→All from the contextual menu. All IEEE 1588 PTP Synchronization-enabled NEs are highlighted.

b. Right-click on the map and choose Highlight→Synchronization→Domain→Freerun/Initial from the contextual menu. All applicable IEEE 1588 PTP Synchronization-enabled NEs are highlighted.

c. Right-click on the map and choose Highlight→Synchronization→Domain→Acquiring from the contextual menu. All applicable IEEE 1588 PTP Synchronization-enabled NEs are highlighted.

d. Right-click on the map and choose Highlight→Synchronization→Domain→Phase Tracking from the contextual menu. All applicable IEEE 1588 PTP Synchronization-enabled NEs are highlighted.

e. Right-click on the map and choose Highlight→Synchronization→Domain→Hold Over from the contextual menu. All applicable IEEE 1588 PTP Synchronization-enabled NEs are highlighted.

f. Right-click on the map and choose Highlight→Synchronization→Domain→Locked from the contextual menu. All applicable IEEE 1588 PTP Synchronization-enabled NEs are highlighted.

3

To remove the path highlights, refer to 7.32 “To manage active highlights on a topology map” (p. 123) .

END OF STEPS

7.17 To create a Source Entry Point between Managed PTP Peers to an unmanaged PTP Peer

7.17.1 General information

This procedure only applies to IEEE 1588 PTP Synchronization-enabled NEs.

Once a Source Entry Point has been created, IP Path Monitors can then be created between it and PTP peers. Source entry points can be used when highlighting PTP Peers in a Sync Domain. See 7.18 “To highlight PTP Peers in a Sync Domain” (p. 109) for more information.

7.17.2 Steps

1

Choose Tools→Synchronization Manager from the NFM-P main menu. The Synchronization Manager form opens.

2

Click on the Add button and then on Source Entry Point from the contextual pop-up. The Source Entry Point (Create) form opens, with the General tab displayed.

3

Configure the parameters, as required:

- Unmanaged IP Address
- Description

- Entry Point 1
- Entry Point 2
- Entry Point 3
- Entry Point 4

Up to four Entry Points may be specified, but Entry Point 1 is required.

4

Click on the Apply button. The Source Entry Point form is refreshed and the PTP Peers tab becomes active.

5

Click on the PTP Peers tab and then click on Search. A list of IEEE 1588 PTP Peers is displayed.

END OF STEPS

7.18 To highlight PTP Peers in a Sync Domain

7.18.1 General information

This procedure only applies to IEEE 1588 PTP Synchronization-enabled NEs.

7.18.2 Steps

1

Choose Tools→Synchronization Manager from the NFM-P main menu. The Synchronization Manager form opens.

2

Click on the Search button. A list of Synchronization Domains (ptp) is displayed.

3

Select the required Synchronization Domain and click on Properties. The Synchronization Domain (Edit) form opens, with the General tab displayed.

4

Click on the PTP Peers tab and then the All sub-tab.

5

Click on the Search button. A list of IEEE 1588 PTP Peers is displayed.

6

Select a PTP Peer entry from the list.

7

Click on the Navigate button and then on IGP View: Highlight PTP Peers(s) from the contextual pop-up.

The IGP Topology map is displayed and the PTP Peers and their paths are highlighted. An information message is also displayed.

8

To remove the path highlights, refer to 7.32 “To manage active highlights on a topology map” (p. 123) .

End of steps

7.19 To highlight the IPv6 shortest path between two routers

7.19.1 Steps

1

Perform one of the following:

a. Choose Tools→Route Analysis→ISIS Topology→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate IGP topology map opens.

b. Choose Tools→Route Analysis→OSPFv3 Topology→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate IGP topology map opens.

2

Press the Ctrl key and click on a source and destination router.

3

Right click and choose Highlight IPv6 SPF from the contextual menu. The IPv6 SPF is highlighted on the topology map.

4

To remove the IPv6 SPF highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

End of steps

7.20 To highlight service tunnels

7.20.1 Steps

1

Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.

2

Choose SDP Binding (Service Tunnel Management) and click Search.

3

Choose one or more SDP bindings and click Navigate→IGP administrative domain.

4

Choose one of the following from the contextual menu:

- IGP View
- ISIS View
- OSPF View

5

Choose one of the following from the contextual menu:

- SDP Binding
- SDP Binding SPF

The SDP binding is highlighted on the map.

Note: The SDP binding is represented by a black dotted line when the tunnel is turned up, and a red dotted line when the tunnel is shut down.

6

To manage or remove the highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

END OF STEPS

7.21 To highlight services

7.21.1 Steps

1

Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.

2

Specify a filter for the search, if required, and click on the Search button. A list of services appears.

3

Choose one or more services and click Navigate→IGP administrative domain.

4

Choose one of the following from the contextual menu:

- IGP View
- ISIS View
- OSPF View

5

Choose one of the following from the contextual menu:

- Service - Seamless MPLS
- Highlight Path to Prefix
- Service SPF - Active SDP binding only
- Service
- Service - Active SDP binding only
- Service SPF
- Highlight Route Target Path

Note: The Highlight Route Target Path option is only available when VPRN services have been chosen.

The service is highlighted on the map.

6

To manage or remove the highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

END OF STEPS

7.22 To highlight composite services

7.22.1 Steps

1

Choose Manage→Composite Services from the NFM-P main menu. The Manage Services form opens.

2

Specify a filter for the search, if required, and click on the Search button. A list of composite services appears.

3

Choose one or more composite services and click on the Navigate button.

4

Choose the IGP administrative domain from the contextual menu.

5

Choose one of the following from the contextual menu:

- IGP View
- ISIS View
- OSPF View

6

Choose one of the following from the contextual menu:

- Composite Service
- Composite Service - Active SDP only
- Composite Service SPF - Active SDP only
- Composite Service SPF

The composite service is highlighted on the map

7

To manage or remove the highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

8

Close the topology map view.

END OF STEPS

7.23 To highlight services from the topology map

7.23.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate topology map appears showing the network objects.

2

Right-click on the map and choose Highlight→Services.

3

Choose one of the following from the contextual menu:

- Service
- Composite Service
- Service - Active SDP only
- Composite Service - Active SDP only
- IES IGP Links
- SDP

The service is highlighted on the map.

4

Configure the filter criteria and click on the Search button. A list of service tunnels is displayed.

5

Choose a service tunnel and click on the OK button. The Find SDP form closes and the service tunnel is highlighted on the map.

6

To manage or remove the highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

7

Close the topology map view.

END OF STEPS

7.24 To highlight a VPRN prefix path

7.24.1 Steps

1

Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.

2

Expand the Services object in the Service (Service Management) drop-down menu and choose VPRN.

3

Specify a filter for the search, if required, and click on the Search button. A list of VPRN services appears.

4

Choose the VPRN service for which you want to highlight the prefix path and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

5

Click on the Navigate button and choose the IGP administrative domain from the contextual menu.

6

Choose IGP View, OSPF View, or ISIS View from the contextual menu.

7

Choose Highlight Prefix from the contextual menu. The Highlight Path to VPRN Prefix form opens.

8

Click on the Select button next to the Site ID parameter to choose the source site in the VPRN. The Select Network Elements form opens.

9

Specify a filter for the search, if required, and click on the Search button. A list of NEs appears.

10

Choose an entry and click on the OK button. The Select Network Elements form closes and the Highlight Path to VPRN Prefix form updates with the source site information.

11

Configure the parameters:

- Prefix Address
- Prefix Length

12

Click on the OK button. The Highlight Path to VPRN Prefix form closes and the VPRN prefix path is highlighted on the map.

13

To manage or remove the highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

14

Close the topology map view.

END OF STEPS

7.25 To highlight IES IGP links

7.25.1 General information

Perform this procedure to search for and highlight network interfaces that are connected to an SDP binding within an IES. IES IGP links are displayed as thin lines on the topology map.

7.25.2 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate topology map appears showing the network objects.

2

Right-click on the map and choose Highlight→Services→IES IGP Link from the contextual menu. The Find IES SDP form opens.

3

Specify a filter for the search, if required, and click on the Search button. A list of IES IGP links appears.

4

Choose an entry and click on the OK button. The Find IES IGP Link form closes and the IES link is highlighted on the map.

5

To manage or remove the highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

6

Close the topology map view.

END OF STEPS

7.26 To highlight historical IP paths

7.26.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu.

The appropriate topology map appears showing the network objects.

2

Right-click on the map and choose Highlight→Paths→IP→Historical SPF from the contextual menu. The Select Historical IP Path Records form opens.

3

Specify a filter for the search, if required, and click on the Search button. A list of historical IP path records appears.

4

Choose an entry and click on the OK button. The Select Historical IP Path Records form closes and the historical IP path is highlighted on the map.

5

To manage or remove the highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

6

Close the topology map.

END OF STEPS

7.27 To highlight LSP paths

7.27.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate topology map appears showing the network objects.

2

Right-click on the map and choose Highlight→Paths→LSP from the contextual menu, then choose one of the following:

a. Choose Active Path to highlight the active path on the topology map.

b. Choose Active Path with LSP Ping to highlight the active path on the topology map and highlight LSP ping test results.

c. Choose Operational Paths to highlight the operational paths on the topology map.

d. Choose Provisioned Path for the Active Path to highlight the provisioned path for the active path on the topology map.

e. Choose Provisioned Paths to highlight the provisioned paths on the topology map.

f. Choose Historical Path to highlight the historical path on the topology map. The Find Historical LSP Path Records form opens. Go to Step 4 .

3

The Select LSP form opens. Perform the following:

1. Click on the Search button.
2. Choose an entry and click on the OK button. The Select LSP form closes and the selected highlights appear on the topology map.
3. Go to Step 6 .

4

Specify a filter for the search, if required, and click on the Search button. A list of historical LSP path records appears.

5

Choose an entry and click on the OK button. The Find Historical LSP Path Records form closes and the historical LSP path is highlighted on the map.

6

To manage or remove the highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

7

Close the topology map.

END OF STEPS

7.28 To highlight S2L LSP paths

7.28.1 Steps

1

Choose Manage→MPLS→Point-to-Multipoint LSPs from the NFM-P main menu. The Manage Point-to-Multipoint LSPs form opens.

2

Click on the Search button. A list of Point-to-Multipoint LSPs is displayed.

3

Select a Point-to-Multipoint LSP from the list and click on the Properties button. The P2MP LSP (Edit) form opens.

4

Click on the S2L Paths tab.

5

Perform one of the following:

a. To navigate to the appropriate topology map from the P2MP LSP (Edit) form, go to Step 6 .

b. To navigate to the appropriate topology map from the S2L Path (Edit) form, go to Step 8 .

6

Select a path from the list and click on the Navigate button.

7

Go to Step 10 .

8

Select a path from the list and click on the Properties button. The S2L Path (Edit) form opens.

9

Click on the Navigate button. If the Navigate button is not visible, click on the More Actions button and choose Navigate.

10

Choose the IGP administrative domain from the contextual menu.

11

Choose one of the following from the contextual menu:

- IGP View
- ISIS View
- MPLS View
- OSPF View

12

Choose one of the following from the contextual menu:

- S2L CSPF Path
- S2L Provisioned Path
- S2L Active Path

The S2L path is highlighted on the map.

13

To manage or remove the highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

14

Close the topology map.

END OF STEPS

7.29 To highlight point-to-multipoint LSPs

7.29.1 Steps

1

Choose Manage→MPLS→Point-to-Multipoint LSPs from the NFM-P main menu. The Manage Point-to-Multipoint LSPs form opens.

2

Click on the Search button. A list of Point-to-Multipoint LSPs is displayed.

3

Select a Point-to-Multipoint LSP from the list and click on the Properties button. The P2MP LSP (Edit) form opens.

4

Click on the Navigate button. If the Navigate button is not visible, click on the More Actions button and choose Navigate.

5

Choose one of the following from the contextual menu:

- OSPF View
- ISIS View
- IGP View
- MPLS View

The Point-to-Multipoint LSP is highlighted on the map. LSPs spanning multiple administrative domains will not be shown in full.

6

To manage or remove the highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

7

Close the topology map.

END OF STEPS

7.30 To highlight point-to-multipoint LSPs from the topology map contextual menu

7.30.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate topology map appears showing the network objects.

2

Right-click on the map and choose Highlight→Paths→P2MP LSPs from the contextual menu, then choose one of the following:

a. Choose Active Path to highlight the active path on the topology map.

b. Choose Active Path with LSP Ping to highlight the active path on the topology map and highlight LSP ping test results.

3

The Select LSP form opens with a list of Point-to-Multipoint LSPs displayed. Choose a Point-to-Multipoint LSP and click on the OK button. The Select LSP form closes and the Point-to-Multipoint LSP is highlighted on the map. LSPs spanning multiple administrative domains will not be shown in full.

4

To manage or remove the highlight, perform 7.32 “To manage active highlights on a topology map” (p. 123) .

5

Close the topology map view.

END OF STEPS

7.31 To perform a highlighted path audit

7.31.1 Steps

1

Create a highlight on a topology map, as described in 7.6 “To highlight the shortest path between two IP addresses” (p. 97) to 7.27 “To highlight LSP paths” (p. 117) .

2

Click on the Legend button at the top of the topology map and choose Highlight Sessions from the contextual menu. The Legend-*topology* form opens with the Highlight Sessions tab displayed.

3

Select and right-click on the highlight that you want to audit and choose Audit→ Path Resource Audit from the contextual menu. The Execute - Path Resource Audit form opens.

4

Configure the Stats Capture Delay (s) parameter.

5

Configure the Threshold parameter for the following audit parameters, if required:

- Utilization
- Interface Error
- Ethernet Error
- Section - Severely Errored Seconds
- Section - Severely Errored Framing Seconds
- Line - Severely Errored Seconds
- Total Drop
- In Profile Drop
- Out of Profile Drop

6

Click on the Execute button to begin the audit. The Execute - Path Resource Audit form closes and the Legend - Topology form reappears.

Note: The audit may take several minutes. The icons on the topology map indicate the audit status. Click on the Icons tab on the Legend - Topology form to view the icon definitions.
To cancel the audit, select and right-click on the highlight for which you want to cancel the audit and choose Cancel Audit from the contextual menu. Alternatively, choose Application→Task manager. The Task Manager form opens. Choose the audit task and click on the OK button to open the Task form. Click on the Cancel Task button and confirm the cancellation.

7

On the Legend - Topology form, right-click on the audited highlighted path and choose Show Audit Results from the contextual menu. The Audit Results form opens.

Note: Alternatively, right-click on a highlighted link and choose Show Audit Results from the contextual menu. The Audit Results form opens with the results from the audit on the highlighted link that you selected.

8

Close the Audit Results form.

9

Clear the audit results, if necessary, by right-clicking on the audited highlighted path on the Legend - Topology form and choosing Clear Audit Results.

10

Close the Legend - Topology form.

11

Close the topology map.

END OF STEPS

7.32 To manage active highlights on a topology map

7.32.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate topology map appears showing the network objects.

2

Click on the Legend button at the top of the topology map and choose Highlight Sessions. The Legend - *Topology_type* - *IGP_Administrative_Domain* form opens with the Highlight Sessions tab displayed.

3

Enable the checkboxes of the highlights you want to view on the topology map. You can click on the Clear All button to disable all of the checkboxes.

4

Click on the Apply button. The selected highlights are displayed on the topology map.

5

Click on the Close button. The Legend - *Topology_type* - *IGP_Administrative_Domain* form closes.

6

Close the topology map view.

END OF STEPS

7.33 To view highlights on a flat map

7.33.1 Steps

1

Create a highlight on a topology map, as described in 7.6 “To highlight the shortest path between two IP addresses” (p. 97) to 7.27 “To highlight LSP paths” (p. 117) .

2

Click on the Legend button at the top of the topology map and choose Highlight Sessions from the contextual menu. The Legend-*topology* form opens with the Highlight Sessions tab displayed.

3

Select and right-click on any highlights that you want to view on a flat map and choose Make Flat Map For Selected Overlay... from the contextual menu. The flat map opens.

4

View the highlights.

5

Close the flat map.

END OF STEPS

7.34 To use the Configure Info Tables button

7.34.1 General information

The Configure Info Tables button is used to create an info table configuration for map objects. See 7.35 “To use the Global Info Tables button” (p. 125) to apply an info table configuration to map objects or the entire map.

7.34.2 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate topology map appears showing the network objects.

2

Click on the Global Info Tables button and choose Configure from the contextual menu. A *topology_view* Info Table Configurations form opens.

3

Click on the Create button. The *topology_view* Info Table Configuration form opens.

4

Enter a name in the Configuration name field.

5

Choose an info table type from the left-hand panel.

6

Click on the check boxes to choose the attributes that you want to display in the info table on the topology map for the associated object.

7

Click on the OK button. The *topology_view* Info Table Configuration form closes.

END OF STEPS

7.35 To use the Global Info Tables button

7.35.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate topology map appears showing the network objects.

2

Click on the Global Info Tables button. A drop-down menu opens with the info table configurations displayed.

3

Choose an info table configuration. The map is refreshed with the corresponding info table displayed next to the map objects.

END OF STEPS

7.36 To apply an info table configuration to a map object

7.36.1 General information

The Global Info Tables menu option allows you to view an info table for a map object, or a group of map objects. See 7.37 “To apply an info table configuration to a map highlight” (p. 126) for information about how to apply an info table to a highlighted object.

An info table configuration must be created before it can be applied to a map object, highlight, or a group of map objects. See 7.34 “To use the Configure Info Tables button” (p. 124) for information about creating an info table.

7.36.2 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate topology map appears showing the network objects.

2

Right-click on a map object or a selection of map objects and choose Selected Info Tables from the contextual menu.

3

Choose one of the following options from the contextual menu:

- a pre-configured info table configuration
- Global
- Off

4

The map view is refreshed with the configured info table displayed next to the map objects.

Note: When you choose the global option from the drop-down menu in Step 3 , the info tables of the selected map objects are refreshed based on Global Info Tables button setting. When you choose the Off option from the drop-down menu in Step 3 , the info tables of the selected map objects are no longer displayed.

End of steps

7.37 To apply an info table configuration to a map highlight

7.37.1 General information

The Global Info Tables menu option allows you to view an info table for a map object, or a group of map objects. See 7.36 “To apply an info table configuration to a map object” (p. 125) for information about how to apply an info table to a map object.

An info table configuration must be created before it can be applied to a map object, highlight, or a group of map objects. See 7.34 “To use the Configure Info Tables button” (p. 124) for information about creating an info table.

7.37.2 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate topology map appears showing the network objects.

2

Click on the Legend button at the top of the topology map and choose Highlight Sessions from the contextual menu. The Legend-*topology* form opens with the Highlight Sessions tab displayed.

Note: You must first create the highlight on the map. For information about how to configure OAM test results highlights, see 13.12 “To highlight the results of a multicast

trace OAM diagnostic on a topology map” (p. 268) to 13.16 “To highlight the results of a multicast trace diagnostic on a topology map from the NFM-P Service Test Manager” (p. 268) .

3

Select and right-click on an entry and choose Highlighted Info Sessions from the contextual menu.

4

Choose one of the following options from the contextual menu:

- a pre-configured info table configuration
- Global
- Off

5

The map view is refreshed with the configured info table displayed next to the map highlights.

END OF STEPS

8 Path and prefix monitoring

8.1 Overview

8.1.1 Path monitoring

You can use the CPAM to monitor registered paths. When a network topology changes, such as a link metric or state change, the system evaluates whether the routes of any registered path are affected. If this is the case, new routes are recorded and CPAM clients are immediately informed. If there is no route for a monitored path as a result of a topology change, a record is logged.

When a monitored path is deleted, the log records for the path are also deleted. Deleted links previously used by the monitored path are not highlighted on the topology map. The CPAM stops monitoring paths when an endpoint router of the path is no longer seen by the CPAM.

The CPAM does not raise an alarm when a monitored path is modified. The initial path and each modified path are recorded and can be reviewed or highlighted on a topology map. The CPAM supports the following types of path monitoring:

- **IP path monitoring**
  Monitors the IP path between two system IP addresses
- **LSP path monitoring**
  Monitors the path (active, secondary, and primary) of an LSP
- **P2MP LSP path monitoring**
  Monitors the path (active, secondary, and primary) of a P2MP LSP

8.1.2 IP path monitoring

The CPAM supports unidirectional and bidirectional IP path monitoring within an IGP administrative domain. Bidirectional IP path monitors determine path divergence and the CPAM raises a self-clearing alarm when the two paths do not share the same set of IP links. If you create two unidirectional IP path monitors instead of a bidirectional path, the CPAM does not monitor path divergence.

You can use the synchronization manager to create unidirectional and bidirectional IP path monitors for PTP peers, and to navigate to and view IP path monitors. See the Synchronization management chapter in the *NSP NFM-P Classic Management User Guide*.

8.1.3 Multicast management and IP path monitoring

There is a correlation between IP path monitoring and a multicast tree. When you configure a multicast tree from a leaf to an RP, from a leaf to a multicast source, or from a multicast source to an RP (depending on the mode of operation—PIM-SM or PIM-SSM), all of the links must be PIM-

enabled. If there is a failure on the path and the IP path switches to a new path, all of the links on the new path must also be PIM-enabled.

To monitor the health of the IP path between the following NEs, you can enable multicast monitoring on the IP path:

- IGMP leaf to RP
- IGMP leaf to source
- source to RP

If multicast monitoring is enabled, the CPAM monitors not only the IP path, but all of the upstream links (from the IGMP leaf to RP or source, or source to RP) to ensure that they are PIM-enabled. The CPAM raises an alarm if a link is not PIM-enabled.

Note: The PIM routers can use different routing tables for multicast, or use different policies for RPF interfaces. If the PIM routers use the unicast routing table without a policy, the multicast management of the IP path on the CPAM ensures that the multicast tree is successfully created and that it stays healthy.

You can view the segments of the route that have multicast enabled by viewing the Segments tab on an IP path record form. See 8.17 “To view IP path records” (p. 159) for information about how to view IP path records.

See 8.3 “To monitor an IP network path” (p. 135) for information about how to enable multicast monitoring.

8.1.4 LSP path monitoring

LSP path monitoring is similar to IP path monitoring. In addition to monitoring the dynamic LSP, the CPAM simultaneously monitors each path of the LSP. Bidirectional LSP path monitors determine path divergence and the CPAM raises a self-clearing alarm when the hops of the active path of the LSP do not match in both directions. If you create two unidirectional LSP path monitors instead of a bidirectional path, the CPAM does not monitor path divergence.

You can select the type of path that the CPAM monitors:

- active
- primary
- secondary with standby option

The CPAM records whether a bypass tunnel is used.

Note: The actual path may not always follow the provisioned path. For example, if fast reroute has occurred, the actual path uses one or more bypass tunnels.

When the LSP is operationally down, a record is created even if there is no actual route. Subsequent connection attempts by RSVP are not logged until the path becomes operational.

You can view historical LSP path monitor statistics when performance statistics collection is enabled in the NFM-P. A statistics collection event is logged after each polling interval. The statistics collection events are displayed on the Events tab of the LSP path monitor form. LSP path records are shown on the Path History tab.

8.1.5 Correlation of path records and routing events

To aid in troubleshooting and root cause analysis, the CPAM provides correlation and navigation from IP and LSP path records to routing events. In the context of path monitoring, routing events are of two types:

- Cause events
- IGP events

Cause events

Cause events are the LSAs that are generated when changes occur in the network. The CPAM records the following LSA types:

- Router LSAs (for OSPF)
- Network LSAs (for OSPF)
- Link State PDUs (for IS-IS)
- TE Link TLV (for GRE and MPLS service tunnels)

Cause event LSAs and PDUs are retrieved from the CPAA LSDB when protocol flags are enabled; see Chapter 4, “Topology management” for information about LSDB updates.

You can navigate from IP and LSP path records to cause events, and from cause events to path records. Viewing cause events correlated with path records allows network troubleshooting at a very granular level. See Stage 10 of 8.2 “Workflow for path and prefix monitoring” (p. 133) for links to procedures.

IGP events

The CPAM analyzes cause event LSAs and produces IGP events that summarize changes in the network. The IGP event function reduces the need for manual examination of individual cause event LSAs. IGP events record the following change types for links:

- Added
- Flapped
- TE Metric changed
- TE Status changed
- Metric changed
- IPv6 Metric changed

The CPAM provides correlation of IP and LSP path records with IGP events. Tabs on the property forms for these records allow quick navigation from:

- IP and LSP path records to correlated IGP events
- IGP events to related IP or LSP path records

Correlation allows you to view the IGP event related to a particular path record, or the path records that result from an IGP event. You can also navigate to highlighted maps of the affected links.

Note: Nokia recommends that you enable BFD on the routing protocol to produce accurate correlation results. The accuracy of correlations also depends on the timing of records in the NFM-P. Some system configurations may not produce up-to-date correlations.

For S2L path monitors, correlation is not supported for IGP events.

8.1.6 BGP prefix monitoring

The CPAA monitors IPv4, IPv6, VPN IPv4, VPN IPv6, and EVPN prefixes in the BGP AS or confederation sub-AS to which it is assigned. The CPAA in the AS or sub-AS reports to the CPAM if one of the monitored routes is added or withdrawn. Neighboring routers send each other update messages to exchange routing information, such as withdrawn routes or preferred paths.

In addition, the CPAA monitors the next hops for each monitored route. A maximum of eight next hops is reported to the CPAM for every monitored route. The CPAA reports any next hop changes for a monitored route to the CPAM. You can retrieve and view this information using the CPAM.

You can configure monitored prefixes on the CPAM for each BGP AS or sub-AS via the GUI or the XML API. See 8.15 “To configure BGP monitored prefixes” (p. 157) for information about how to configure monitored prefixes using the GUI.

If you configure threshold reaching alarms, the CPAM raises an alarm for all of the actively monitored routes in each BGP AS when the CPAM detects route flapping — routes that appear and disappear, or changing next hops. You can manually clear the alarms. The CPAA clears the alarms when the flapping stops. You can specify the flapping rate threshold within an interval for which the CPAM raises an alarm.

In addition, the CPAM raises the BGP Monitored Prefix Unreachable alarm when a BGP route to a monitored prefix is not found by the CPAA. You can suppress these alarms for each monitored BGP prefix. See 16.3 “To configure alarm thresholds” (p. 295) for information about how to configure the alarm.

8.1.7 GNE support

The CPAM supports the limited management of GNEs. The CPAM support of GNEs requires the proper MIB support on GNEs.

Note: Standard MIBs support read-only mode for the path objects. LSPs or paths can not be configured from the NFM-P.

The NFM-P mediation engine supports standard MPLS MIBs. The GNEs managed by the NFM-P using standard MIBs must use attributes, IDs and traps in a specific manner to ensure proper operation. Otherwise, LSP objects may be represented incorrectly in the NFM-P.

See Appendix A, “CPAM MIB support for GNEs” for information about MIB support. See “To prepare a GNE for NFM-P management” in the *NSP NFM-P Classic Management User Guide* for information about how to add a routing MIB to a GNE profile.

8.2 Workflow for path and prefix monitoring

8.2.1 Stages

1

Determine the map type you want to view:

- maps that show the topology
- maps that show protocol-specific topologies

2

Enable NFM-P performance statistics collection for IP and MPLS interfaces, and for LSPs. Configure the MIB entry policy for the required statistics object type, or class; see the procedure "To configure polling for a MIB statistics class" in the *NSP NFM-P Statistics Management Guide*. Set the Administrative State parameter in the MIB entry policy to Up.

- For network interfaces, enable the Ip Interface Stats object type on the Network Interface properties form. The MIB entry name is vRtrIfStatsEntry.
- For MPLS interfaces, enable MPLS Interface Stats on the MPLS Interface properties form. The MIB entry name is vRtrMplsIfStatEntry.
- For LSP utilization, enable the MPLS LSP Egress Stats object type on the Dynamic LSP properties form for each LSP. The MIB entry name is vRtrMplsLspStatisticsEntry.

Set the polling interval to less than one hour.

3

For LSP utilization history: on the Accounting tab of the Dynamic LSP properties form for each LSP, assign an accounting policy and set the Administrative State to Up. See the procedure "To create a Dynamic LSP" in the *NSP NFM-P Classic Management User Guide*.

4

Configure monitoring, as required.

- Monitor an IP network path. See 8.3 "To monitor an IP network path" (p. 135) for more information.
- Create an IP path monitor between two routers on a topology map. See 8.9 "To create an IP path monitor between two routers on a topology map" (p. 147) for more information
- Monitor a bidirectional IP network path. See 8.4 "To monitor a bidirectional IP network path" (p. 137) for more information.
- Create a bidirectional IP path monitor from a unidirectional IP path monitor. See 8.10 "To create a bidirectional IP path monitor from a unidirectional IP path monitor" (p. 149) for more information.
- Monitor an LSP. See 8.5 "To monitor a dynamic LSP" (p. 139) for more information.
- Create an LSP path monitor from an NFM-P-managed dynamic LSP. See 8.11 "To create an LSP path monitor from a dynamic LSP" (p. 150) for more information.

- Create LSP path monitors for multiple LSP paths. See 8.12 “To create LSP path monitors for multiple LSP paths” (p. 153) for more information.
- Monitor a bidirectional LSP path. See 8.6 “To monitor a bidirectional LSP path” (p. 141) for more information.
- Monitor a P2MP LSP. See 8.7 “To monitor a P2MP LSP” (p. 143) for more information.
- Create a P2MP LSP path monitor from an NFM-P-managed P2MP LSP . See 8.13 “To create a P2MP LSP path monitor from a P2MP LSP” (p. 154) for more information.
- Monitor an SDP tunnel. See 8.8 “To monitor an SDP tunnel” (p. 145) for more information.
- Create path monitors for multiple service tunnels. See 8.14 “To create path monitors for multiple service tunnels” (p. 156) for more information.
- Configure BGP monitored prefixes. See 8.15 “To configure BGP monitored prefixes” (p. 157) for more information.

5

Create a size constraint policy to specify the maximum number of historical path records that the CPAM retains, if required. See 8.16 “To configure the size constraint limit for path monitor records” (p. 158) for more information.

6

View path records and historical path records, as required

- View IP path records of all of the monitored paths. See 8.17 “To view IP path records” (p. 159) for more information.
- View LSP path records of all of the monitored paths. See 8.18 “To view LSP path records” (p. 160) for more information.
- View path records of all of the monitored 2SL paths. See 8.19 “To view S2L path records” (p. 162) for more information.
- View the historical path records of a monitored LSP path binding. See 8.20 “To view historical path records of a monitored LSP path binding” (p. 164) for more information.
- Delete historical path records, as required. See 8.31 “To delete historical events” (p. 175) for more information.

7

View status change history of monitored prefixes, if required. See 8.21 “To view status change history of monitored prefixes” (p. 165) for more information.

8

View the total cost of IP paths and IP path segments, if required. See 8.22 “To view the total cost of IP paths and IP path segments” (p. 166) for more information.

9

Navigate to a dynamic LSP or a monitored path on a topology map, if required. See 8.23 “To navigate to a dynamic LSP on a topology map” (p. 167) and 8.24 “To navigate to a monitored path on a topology map” (p. 168) for more information.

10

Determine the cause event of an IP or LSP path record, as required. Alternatively, navigate from a cause event to the IP or LSP path record of the monitored path, or navigate to the cause event of a path record of GRE or MPLS service tunnels.

- Find the cause event of an IP or LSP path record. See 8.25 “To find the cause event of an IP or LSP path record” (p. 169) for more information.
- Find the cause event of a path record of a service tunnel. See 8.26 “To find the cause event of a path record of a service tunnel” (p. 170) for more information.
- Find the IP or LSP path monitor record associated with a cause event. See 8.27 “To find the IP or LSP path monitor record associated with a cause event” (p. 171) for more information.

11

Sort records, as required.

- Sort IP path records by error code. See 8.28 “To sort IP path records by error code” (p. 172) for more information.
- Sort LSP path records by error code. See 8.29 “To sort LSP path records by error code” (p. 173) for more information.
- Sort LSP path records by last reroute cause. See 8.30 “To sort LSP path records by last reroute cause” (p. 174) for more information.

8.3 To monitor an IP network path

8.3.1 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

Note: You can also create an IP path monitor from the topology map. See 8.9 “To create an IP path monitor between two routers on a topology map” (p. 147) for information.

2

Click on the Create button and choose IP Path Monitor. The IP Path Monitor (Create) form opens with the General tab displayed.

3

Configure the parameters:

- Name
- Description
- Monitor State

4

Configure the Source IP parameter or use the Select button to choose a source router.

5

Configure the Source Length parameter.

6

Configure the Destination IP parameter or use the Select button to choose a destination router.

7

Configure the Destination Length parameter.

8

Configure the Monitor Multicast parameter.

9

Click on the Auto OAM tab button. The General tab is displayed.

10

Click on the Select button in the STM Policy panel to associate a test policy to the IP path monitor. The Select STM Policy - IP Path Monitor form opens.

11

Click on the Search button. A list of configured test policies appears.

12

Choose an entry and click on the OK button. The Select STM Policy - IP Path Monitor form closes.

13

Click on the Select button in the Execution Policy panel to associate an execution policy to the IP path monitor. The Select Execution Policy - IP Path Monitor form opens.

14

Click on the Search button. A list of configured execution policies appears.

15

Choose an entry and click on the OK button. The Select Execution Policy - IP Path Monitor form closes.

Note: See 13.9 “To configure an OAM test execution policy” (p. 261) for information about how to create an execution policy.
See 13.10 “To manually run an OAM diagnostic on an IP, LSP, or P2MP path monitor” (p. 262) for information about how to run an OAM test.

16

Click on the Apply button to save the configuration. The CPAM monitors the path only if the Monitor State parameter is set to Up.

17

Click on the Path History tab button to view monitored IP paths.

Note: You can click on the Capture Path button to perform an immediate path capture.

18

Click on the Service Tunnels tab button to view monitored GRE and LDP tunnels.

19

Click on the Services tab button to view services that use the monitored IP paths.

20

Click on the Composite Services tab button to view composite services that use the monitored IP paths.

21

Close the IP Path Monitor (Create) form.

22

Close the Path and Prefix Monitoring form.

END OF STEPS

8.4 To monitor a bidirectional IP network path

8.4.1 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

2

Click on the Create button and choose Bidirectional IP Path Monitor. The Bidirectional IP Path Monitor (Create) form opens with the General tab displayed.

Note: Alternatively, you can create a bidirectional IP network path monitor from an existing unidirectional path monitor. See 8.10 “To create a bidirectional IP path monitor from a unidirectional IP path monitor” (p. 149) .
You can also create a bidirectional IP path monitor from the topology map. See 8.9 “To create an IP path monitor between two routers on a topology map” (p. 147) for information.

3

Configure the parameters:

- Name
- Description
- Monitor State

4

Configure the Endpoint A IP parameter or use the Select button to choose a router.

5

Configure the Endpoint A Length parameter.

6

Configure the Endpoint A IP parameter or use the Select button to choose a router.

7

Configure the Endpoint A Length parameter.

8

Click on the Apply button to save the configuration. The CPAM monitors the path only if the Monitor State is set to Up. Unidirectional paths are created, if required, or existing unidirectional paths with matching endpoints are associated with the new bidirectional path.

9

Click on the Path History tab button to view historical paths of the two unidirectional paths. You can sort the list by the time at which the paths were rerouted, created, or removed.

Note: You can click on the Capture Path button to perform an immediate path capture. See 13.10 “To manually run an OAM diagnostic on an IP, LSP, or P2MP path monitor” (p. 262) Chapter 13, “OAM diagnostics” for information about how to run an OAM test.

10

Click on the Service Tunnels tab button to view monitored GRE and LDP SDP tunnels in both directions.

11

Click on the Services tab button to view services that use the monitored IP paths.

12

Click on the Composite Services tab button to view composite services that use the monitored IP paths.

13

Close the Bidirectional IP Path Monitor (Create) form.

14

Close the Path and Prefix Monitoring form.

END OF STEPS

8.5 To monitor a dynamic LSP

8.5.1 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

2

Click on the Create button and choose LSP Monitor. The LSP Path Monitor (Create) form opens with the General tab displayed.

Note: Alternatively, you can create an LSP path monitor from the properties form of an NFM-P-managed dynamic LSP. See 8.11 “To create an LSP path monitor from a dynamic LSP” (p. 150) for information.

3

Configure the parameters:

- Name
- Description
- Monitor State

4

To select the required dynamic LSP, click select and choose the LSP from the list.

5

Configure the Path Types parameter.

Nokia recommends that you choose the Active option.

6

Click on the Auto OAM tab button. The General tab is displayed.

7

Click on the Select button in the STM Policy panel to associate a test policy to the IP path monitor. The Select STM Policy - LSP Path Monitor form opens.

8

Click on the Search button. A list of configured test policies appears.

9

Choose an entry and click on the OK button. The Select STM Policy - LSP Path Monitor form closes.

10

Click on the Select button in the Execution Policy panel to associate an execution policy to the LSP monitor. The Select Execution Policy - LSP Path Monitor form opens.

11

Click on the Search button. A list of configured execution policies appears.

12

Choose an entry and click on the OK button. The Select Execution Policy - LSP Path Monitor form closes.

Note: See 13.9 “To configure an OAM test execution policy” (p. 261) Chapter 13, “OAM diagnostics” for information about how to create an execution policy.
See 13.10 “To manually run an OAM diagnostic on an IP, LSP, or P2MP path monitor” (p. 262) Chapter 13, “OAM diagnostics” for information about how to run an OAM test.

13

Click on the Apply button to save the configuration. The CPAM monitors the path only if the Monitor State is set to Up.

14

Click on the Path History tab to view LSP path records. See 8.18 “To view LSP path records” (p. 160).

Note: You can click on the Capture Path button to perform an immediate path capture.

15

Click on the Service Tunnels tab button to view monitored GRE and LDP SDP tunnels in both directions.

16

Click on the Services tab button to view services that use the monitored LSP paths.

17

Click on the Composite Services tab button to view composite services that use the monitored LSP paths.

18

Click on the Events tab to view LSP path monitor statistics.

The frequency of collection events depends on the polling interval set in the MPLS LSP Egress Stats MIB entry policy. Each LSP path monitor statistics record shows the LSP Byte change and active LSP path for a given polling interval.

You can configure retention times for Event records. Click on the Edit Policy button and configure the Event Retention Time parameter on the Event Policy (Edit) form.

You can purge all event records for LSP path monitor statistics. Click on the Edit Policy button, then click Purge Event Records on the Event Policy form. All LSP path monitor statistics are cleared from the table until the next event record arrives.

For long retention times, ensure that the system has sufficient physical disk space. Use the following formula as a guide to estimating the additional disk space required (in MB) for the NFM-P Database /opt/nsp/nfmp/db/tablespace partition:

Number of LSPs monitored / Polling interval (minutes) x Retention time (hours) x 0.024375

19

Close the LSP Path Monitor (Create) form.

20

Close the Path and Prefix Monitoring form.

END OF STEPS

8.6 To monitor a bidirectional LSP path

8.6.1 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

2

Click on the Create button and choose Bidirectional LSP Path Monitor. The Bidirectional IP Path Monitor (Create) form opens with the General tab displayed.

3

Configure the parameters:

- Name
- Description
- Monitor State

4

Configure the Endpoint A IP parameter or use the Select button to choose a router.

5

Configure the Endpoint A Length parameter.

6

Configure the Endpoint A IP parameter or use the Select button to choose a router.

7

Configure the Endpoint A Length parameter.

8

Configure the ID parameter in the LSP A panel.

9

Configure the ID parameter in the LSP B panel.

10

Click on the Apply button to save the configuration. The CPAM monitors the path only if the Monitor State is set to Up. Unidirectional paths are created, if required, or existing unidirectional paths with matching endpoints are associated with the new bidirectional path.

11

Click on the Path History tab button to view historical paths of the two unidirectional paths. You can sort the list by the time at which the paths were rerouted, created, or removed.

Note: You can click on the Capture Path button to perform an immediate path capture. See 13.10 “To manually run an OAM diagnostic on an IP, LSP, or P2MP path monitor” (p. 262) for information about how to run an OAM test.

12

Click on the Service Tunnels tab button to view monitored GRE and LDP SDP tunnels in both directions.

13

Close the Bidirectional LSP Path Monitor (Create) form.

14

Close the Path and Prefix Monitoring form.

END OF STEPS

8.7 To monitor a P2MP LSP

8.7.1 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

2

Click on the Create button and choose P2MP LSP Path Monitor. The P2MP LSP Path Monitor (Create) form opens with the General tab displayed.

3

Configure the parameters:

- Name
- Description
- Monitor State

4

Configure the ID parameter in the LSP panel.

5

Click on the Apply button to save the configuration. The CPAM monitors the path only if the Monitor State is set to Up.

6

Click on the Auto OAM tab button. The General tab is displayed.

7

Click on the Select button in the STM Policy panel to associate a test policy to the IP path monitor. The Select STM Policy - LSP Path Monitor form opens.

8

Click on the Search button. A list of configured test policies appears.

9

Choose an entry and click on the OK button. The Select STM Policy - LSP Path Monitor form closes.

10

Click on the Select button in the Execution Policy panel to associate an execution policy to the P2MP LSP monitor. The Select Execution Policy - P2MP LSP Path Monitor form opens.

11

Click on the Search button. A list of configured execution policies appears.

12

Choose an entry and click on the OK button. The Select Execution Policy - P2MP LSP Path Monitor form closes.

Note: See 13.9 “To configure an OAM test execution policy” (p. 261) for information about how to create an execution policy.
See 13.10 “To manually run an OAM diagnostic on an IP, LSP, or P2MP path monitor” (p. 262) or information about how to run an OAM test.

13

Click on the S2L Paths tab button to view monitored S2L paths.

Note: You can click on the Capture Path button to perform an immediate path capture.

14

Click on the Path History tab button to view monitored IP paths.

Note: You can click on the Capture Path button to perform an immediate path capture. If the Capture Path button is not visible, click on the More Actions button and choose Capture Path.

15

Close the P2MP LSP (Create) form.

16

Close the Path and Prefix Monitoring form.

END OF STEPS

8.8 To monitor an SDP tunnel

8.8.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate topology map appears showing the network objects.

2

Right-click on the topology map and choose Highlight SDP from the contextual menu. The Find SDP form opens.

3

Configure the filter criteria and click on the Search button. A list of service tunnels is displayed.

4

Select a service tunnel in the list and click on the Properties button. The Tunnel (Edit) form opens with the General tab displayed.

5

Click on the Create/Edit Path Monitor button. The IP Path Monitor (Create) form opens with the General tab displayed.

Note: If a path monitor already exists for the service tunnel, the IP Path Monitor (Edit) form opens with the General tab displayed.

6

Configure the parameters, if required:

- Name
- Description
- Monitor State

Note: The Source IP, Source Length, Destination IP, and Destination Length parameters are automatically configured with the system IP address of the site and default length.

7

Click on the Apply button.

8

To create a bidirectional IP path monitor, click on the Create Bidirectional IP Path Monitor button. The Bidirectional IP Path Monitor (Create) form opens with the General tab displayed. Perform Step 3 to Step 13 of 8.4 “To monitor a bidirectional IP network path” (p. 137) .

9

Click on the Path History tab button to view monitored IP paths.

10

Click on the Service Tunnels tab button to view monitored GRE and LDP tunnels.

11

Close the IP Path Monitor (Edit) form. The Tunnel (Edit) form reappears.

12

To navigate to a service tunnel on the topology map, perform the following:

1. Click on the Navigate button.
2. Choose one of the following views:
   - IGP View
   - ISIS View
   - OSPF View
3. Choose the IGP administrative domain in which you want to view the SDP. A dialog box appears.
4. Click on the OK button.
5. The Discovered L3 Objects form opens.
6. Select all of the entries in the list and drag and drop them onto the topology map.
7. Click on the Subnets tab button on the Discovered L3 Objects form.
8. Select all of the entries in the list and drag and drop them onto the topology map.
9. Click on the Auto-layout button, if required. A dialog box appears.
10. Click on the Yes button. The dialog box closes.
11. Click on the Legend button at the top of the topology map and choose Highlight Sessions from the contextual menu. The Legend - *Topology_type* - *IGP_Administrative_Domain* form opens with the Highlight Sessions tab displayed.
12. Enable the checkboxes of the highlights you want to view on the topology map. You can click on the Clear All button to disable all of the checkboxes.

13. Click on the Apply button. The selected highlights are displayed on the topology map.
14. Click on the Close button. The Legend - *Topology_type* - *IGP_Administrative_Domain* form closes.
15. Close the topology map view.
16. Close the Tunnel (Edit) form.
17. Close the Manage Service Tunnels form.

END OF STEPS

8.9 To create an IP path monitor between two routers on a topology map

8.9.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate topology map appears showing the network objects.

2

Click on the source router.

3

Press the Ctrl key and click on the destination router.

4

Right-click on the map and choose Create IP Path Monitor from the contextual menu. The IP Path Monitor (Create) form opens with the General tab displayed.

5

Configure the parameters:

- Name
- Description
- Monitor State

6

Configure the Source Length parameter.

7

Configure the Destination Length parameter.

8

Click on the Auto OAM tab button. The General tab is displayed.

9

Click on the Select button in the STM Policy panel to associate a test policy to the IP path monitor. The Select STM Policy - IP Path Monitor form opens.

10

Click on the Search button. A list of configured test policies appears.

11

Choose an entry and click on the OK button. The Select STM Policy - IP Path Monitor form closes.

12

Click on the Select button in the Execution Policy panel to associate an execution policy to the IP path monitor. The Select Execution Policy - IP Path Monitor form opens.

13

Click on the Search button. A list of configured execution policies appears.

14

Choose an entry and click on the OK button. The Select Execution Policy - IP Path Monitor form closes.

Note: See 13.9 “To configure an OAM test execution policy” (p. 261) for information about how to create an execution policy.
See 13.10 “To manually run an OAM diagnostic on an IP, LSP, or P2MP path monitor” (p. 262) for information about how to run an OAM test.

15

Click on the Apply button to save the configuration. The CPAM monitors the path only if the Monitor State is set to Up.

16

Click on the Path History tab button to view monitored IP paths.

Note: You can click on the Capture Path button to perform an immediate path capture.

17

Click on the Service Tunnels tab button to view monitored GRE and LDP SDP tunnels in both directions.

18

Click on the Services tab button to view services that use the monitored IP paths.

19

Click on the Composite Services tab button to view composite services that use the monitored IP paths.

20

Close the IP Path Monitor (Create) form.

21

Close the topology map.

END OF STEPS

8.10 To create a bidirectional IP path monitor from a unidirectional IP path monitor

8.10.1 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

2

Configure the list filter criteria and choose IP Path Monitor (Monitored Path) from the object menu.

3

Click on the Search button. A list of IP path monitors appears.

4

Choose an entry and click on the Properties button. The IP Path Monitor (Edit) form opens with the General tab displayed.

5

Click on the Create Bidirectional IP Path Monitor button. The Bidirectional IP Path Monitor (Create) form opens with the General tab displayed.

6

Configure the parameters:

- Name
- Description
- Monitor State

7

Click on the Apply button to save the configuration. The CPAM monitors the path only if the Monitor State is set to Up. Unidirectional paths are created, if required, or existing unidirectional paths with matching endpoints are associated with the new bidirectional path.

8

Click on the Path History tab button to view historical paths of the two unidirectional paths. You can sort the list by the time at which the paths were rerouted, created, or removed.

Note: You can click on the Capture Path button to perform an immediate path capture. See 13.10 “To manually run an OAM diagnostic on an IP, LSP, or P2MP path monitor” (p. 262) Chapter 13, “OAM diagnostics” for information about how to run an OAM test.

9

Click on the Service Tunnels tab button to view monitored GRE and LDP SDP tunnels in both directions.

10

Click on the Services tab button to view services that use the monitored IP paths.

11

Click on the Composite Services tab button to view composite services that use the monitored IP paths.

12

Close the Bidirectional IP Path Monitor (Create) form.

13

Close the IP Path Monitor (Edit) form.

14

Close the Path and Prefix Monitoring form.

END OF STEPS

8.11 To create an LSP path monitor from a dynamic LSP

8.11.1 Purpose

Perform this procedure to create an LSP path monitor from an NFM-P-managed dynamic LSP properties form.

8.11.2 Steps

1

Choose Manage→MPLS→Dynamic LSPs from the NFM-P main menu. The Manage Dynamic LSPs form appears.

2

Specify a filter for the search, if required, and click on the Search button. A list of Dynamic LSPs appears.

3

Select a Dynamic LSP, click on the Monitor button, and choose Create LSP Monitor from the contextual menu. A dialog box appears indicating the number of monitors that may be created or that may exist.

4

Click on the OK button. The dialog box closes and the Select Path Types dialog box appears.

5

Choose the path types that you want to monitor and click on the OK button. The Select Path Types dialog box closes.

6

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

7

Click on the View LSP Monitor button. If the button is not visible, click on the More Actions button and choose LSP Monitor. The LSP Path Monitor (Edit) form opens with the General tab displayed.

8

Configure the parameters:

- Description
- Monitor State
- Path Types

9

Click on the Auto OAM tab button. The General tab is displayed.

10

Click on the Select button in the STM Policy panel to associate a test policy to the IP path monitor. The Select STM Policy - LSP Path Monitor form opens.

11

Click on the Search button. A list of configured test policies appears.

12

Choose an entry and click on the OK button. The Select STM Policy - LSP Path Monitor form closes.

13

Click on the Select button in the Execution Policy panel to associate an execution policy to the LSP monitor. The Select Execution Policy - LSP Path Monitor form opens.

14

Click on the Search button. A list of configured execution policies appears.

15

Choose an entry and click on the OK button. The Select Execution Policy - LSP Path Monitor form closes.

Note: See 13.9 “To configure an OAM test execution policy” (p. 261) for information about how to create an execution policy.
See 13.10 “To manually run an OAM diagnostic on an IP, LSP, or P2MP path monitor” (p. 262) for information about how to run an OAM test.

16

Click on the Apply button to save the configuration. The CPAM monitors the path only if the Monitor State is set to Up.

17

Click on the Path History tab to view monitored LSP paths.

Note: You can click on the Capture Path button to perform an immediate path capture.

18

Click on the Events tab to view LSP path monitor statistics.

The frequency of collection events depends on the polling interval set in the MPLS LSP Egress Stats MIB entry policy. Each LSP path monitor statistics record shows the LSP Byte change and active LSP path for a given polling interval.

You can configure retention times for Event records. Click on the Edit Policy button and configure the Event Retention Time parameter on the Event Policy (Edit) form.

You can purge all event records for LSP path monitor statistics. Click on the Edit Policy button, then click Purge Event Records on the Event Policy form. All LSP path monitor statistics are cleared from the table until the next event record arrives.

For long retention times, ensure that the system has sufficient physical disk space. Use the following formula as a guide to estimating the additional disk space required (in MB) for the NFM-P Database /opt/nsp/nfmp/db/tablespace partition:

Number of LSPs monitored / Polling interval (minutes) x Retention time (hours) x 0.024375

19

Click on the Service Tunnels tab to view SDP tunnels using MPLS-RSVP and using the monitored LSP in both directions.

20

Click on the Services tab to view services that use the monitored LSP paths.

21

Click on the Composite Services tab to view composite services that use the monitored LSP paths.

22

Close the LSP Path Monitor (Edit) form.

23

Close the Dynamic LSP (Edit) form.

24

Close the Manage Dynamic LSPs form.

END OF STEPS

8.12 To create LSP path monitors for multiple LSP paths

8.12.1 Steps

1

Choose Manage→MPLS→Dynamic LSPs from the NFM-P main menu. The Manage Dynamic LSPs form appears.

2

Specify a filter for the search, if required, and click on the Search button. A list of Dynamic LSPs appears.

3

Using the Ctrl key, select the Dynamic LSPs that you want to monitor.

Note: The CPAM creates a path monitor only for the Dynamic LSPs that do not already have a path monitor.

4

Click on the Monitor button and choose Create LSP Monitor from the contextual menu. A dialog box appears indicating the number of monitors that may be created or that may exist.

5

Click on the OK button. The dialog box closes and the Select Path Types dialog box appears.

6

Choose the path types that you want to monitor and click on the OK button. The Select Path Types dialog box closes and the CPAM creates administratively enabled path monitors.

7

To view the path monitors, perform the following:

1. Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.
2. Choose LSP Path Monitor (Monitored Path) from the object menu.
3. Click on the Search button. The LSP path monitors are listed.
4. Close the Path and Prefix Monitoring form.

8

Close the Manage Dynamic LSPs form.

END OF STEPS

8.13 To create a P2MP LSP path monitor from a P2MP LSP

8.13.1 Steps

1

Choose Manage→MPLS→P2MP LSPs from the NFM-P main menu. The Manage Point-to-Multipoint LSPs form appears.

2

Specify a filter for the search, if required, and click on the Search button. A list of Point-to-Multipoint LSPs appears.

3

Select a Point-to-Multipoint LSP and click on the Create LSP Monitor button. A dialog box appears indicating the number of monitors that may be created or that may exist.

4

Click on the OK button.

5

Click on the Properties button. The P2MP LSP (Edit) form opens with the General tab displayed.

6

Click on the More Actions button and choose View LSP Monitor. The LSP Path Monitor (Edit) form opens with the General tab displayed.

7

Configure the parameters:

- Description
- Monitor State

8

Click on the Auto OAM tab button. The General tab is displayed.

9

Click on the Select button in the STM Policy panel to associate a test policy to the IP path monitor. The Select STM Policy - LSP Path Monitor form opens.

10

Click on the Search button. A list of configured test policies appears.

11

Choose an entry and click on the OK button. The Select STM Policy - LSP Path Monitor form closes.

12

Click on the Select button in the Execution Policy panel to associate an execution policy to the LSP monitor. The Select Execution Policy - LSP Path Monitor form opens.

13

Click on the Search button. A list of configured execution policies appears.

14

Choose an entry and click on the OK button. The Select Execution Policy - LSP Path Monitor form closes.

Note: See 13.9 “To configure an OAM test execution policy” (p. 261) for information about how to create an execution policy.
See 13.10 “To manually run an OAM diagnostic on an IP, LSP, or P2MP path monitor” (p. 262) or information about how to run an OAM test.

15

Click on the S2L Paths tab button to view monitored S2L paths.

Note: You can click on the Capture Path button to perform an immediate path capture.

16

Click on the Path History tab button to view monitored IP paths.

Note: You can click on the Capture Path button to perform an immediate path capture. If the Capture Path button is not visible, click on the More Actions button and choose Capture Path.

17

Close the LSP Path Monitor (Edit) form.

18

Close the P2MP LSP (Edit) form.

19

Close the Manage Point-to-Multipoint LSPs form.

END OF STEPS

8.14 To create path monitors for multiple service tunnels

8.14.1 Steps

1

Choose Manage→Service Tunnels from the NFM-P main menu. The Manage Service Tunnels form appears.

2

Specify a filter for the search, if required, and click on the Search button. A list of service tunnels appears.

3

Using the Ctrl key, choose the service tunnels that you want to monitor.

4

Click on the Monitor button and choose one of the following:

- Create IP Path Monitor
- Create Bidirectional Path Monitor

A dialog box appears.

5

Click on the Yes button. The dialog box closes and the CPAM creates administratively enabled path monitors.

Note: The CPAM creates a path monitor only for those GRE or LDP-enabled service tunnels that do not have a path monitor.

6

To view a path monitor, perform the following:

1. Choose a service tunnel and click on the Properties button. The Tunnel (Edit) form opens with the General tab displayed.
2. Click on the Create/Edit Path Monitor button. The IP Path Monitor (Edit) form opens with the General tab displayed.
3. View information on the following tabs:
   - Path History
   - Service Tunnels
   - Faults
4. Close the IP Path Monitor (Edit) form.
5. Close the Tunnel (Edit) form.

7

Close the Manage Service Tunnels form.

END OF STEPS

8.15 To configure BGP monitored prefixes

8.15.1 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

2

Click on the Create button and choose Create BGP Monitor Prefix from the contextual menu. The BGP Monitor Prefix (Create) form opens with the General tab displayed.

3

Click on the Select button in the BGP AS panel. The Select BGP AS - BGP Monitored Prefix form opens.

4

Configure a filter for the search, if required, and click on the Search button. A list of BGP AS appears.

5

Select a BGP AS and click on the OK button. The Select BGP AS - BGP Monitored Prefix form closes.

6

Configure the parameters:

- Name
- Description
- IP Address
- Prefix Length
- Address Type
- Monitor State
- Route Distinguisher Type
- Route Distinguisher

The Route Distinguisher Type parameter and Route Distinguisher parameter are configurable only when the Address Type parameter is set to VPN IPv4 or VPN IPv6.

7

Configure the alarm threshold parameters, if required.

- Suppress Alarms
- Override Alarm Thresholds
- AS Path Length Threshold
- Redundancy Loss Threshold

Note: See 16.3 “To configure alarm thresholds” (p. 295) for information about how to configure alarm thresholds.
You can only configure these alarm threshold parameters if the related alarm threshold is configured for the CPAA managing the BGP AS.

8

Click on the OK button. The BGP Monitored Prefix (Create) form closes.

9

Close the Path and Prefix Monitoring form.

END OF STEPS

8.16 To configure the size constraint limit for path monitor records

8.16.1 Before you begin

Configuring the path monitor record size constraint option allows you to define the disk space allocated to historical path monitor (LSP/IP) data that is stored within the system. When the size constraint limit is reached, the CPAM deletes the oldest records to make room for the most recent records.

For production networks where the total number of combined IP/LSP path monitors created within the system is less than 5000, Nokia recommends using the size constraint default setting of 1024 MB.

Where more than 5000 combined (IP/LSP) monitors are created within one system, Nokia recommends setting the path monitor record size constraint to 10240 MB.

A minimum configurable size constraint of 128 MB is provided for lab testing purposes for small networks with approximately 10 NEs, where only a few hundred combined path monitors are created within a system.

8.16.2 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

2

Click on the Size Constraint button. The MonitoredPathManager - monitor-path-mgr (Edit) form opens.

3

Configure the Path Monitor Record Size Constraint parameter.

4

Click on the OK button. A dialog box appears.

5

Click on the Yes button. The dialog box and the MonitoredPathManager - monitor-path-mgr (Edit) form close.

6

Close the Path and Prefix Monitoring form.

END OF STEPS

8.17 To view IP path records

8.17.1 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

2

Choose IP Path Record (Monitored Path) from the object menu and click on the Search button. A list of IP path records appears.

3

Choose an entry and click on the Properties button. The IP Path Record (Edit) form opens with the General tab displayed.

4

View the following information:

- record time
- monitor error code
- details of the error
- route type
- source IP address and length
- destination IP address and length
- total cost calculation indicator

5

Click on the Total Cost tab to view the total cost calculation.

6

Click on the Segments tab button to view the information about route segments, which includes:

- segment ID
- start segment indicator
- internal segment indicator
- end segment indicator
- link type
- protocol
- IGP shortcut part
- multicast-enabled indicator
- start router ID
- start egress IP address
- end ingress IP address
- end router ID
- cost

7

Click on the IGP Events tab to view IGP events correlated with the IP path record.

8

Close the IP Path Record (Edit) form.

9

Close the Path and Prefix Monitoring form.

END OF STEPS

8.18 To view LSP path records

8.18.1 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

2

Choose one of the following from the object menu:

- LSP Path Record (Monitored Path)
- P2MP LSP Path Record (Monitored Path)

3

Click on the Search button. A list of records appears.

4

Choose a record and click on the Properties button. The LSP Path Record (View) form opens.

5

View the following information:

- record time
- monitor error cause
- last reroute cause
- LSP monitor
- LSP path state and LSP path operating state
- LSP path type
- bypass path active
- detour active
- MPLS path name and ID
- failure code

6

Click on the Path Segments tab.

7

Click Search and choose an entry.

8

Click Properties. The Path Segment (Edit) form opens.

9

View the segment details.

10

Close the Path Segment (Edit) form.

11

Click on the IGP Events tab to view IGP events correlated with the LSP path record.

12

Close the LSP Path Record (Edit) form.

13

Close the Path and Prefix Monitoring form.

END OF STEPS

8.19 To view S2L path records

8.19.1 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

2

Choose S2L Path Record from the object menu.

3

Click on the Search button. A list of records appears.

4

Choose a record and click on the Properties button. The S2L Path Monitor (Edit) form opens with the General tab displayed.

5

Click on the Properties button in the S2L Path panel. The S2L Path (Edit) form opens.

6

Click on the Provision Path tab button to view the provisioned path.

7

Click on the Actual Path tab button to view the actual path.

8

Click on the CSPF Path tab button to view the CSPF path.

9

Close the S2L Path (Edit) from.

10

Click on the Path History tab button.

11

Click on the Search button. A list of records appears.

12

Choose a record and click on the Properties button. The LSP Path Record (Edit) form opens with the General tab displayed.

13

View the following information:

- record time
- monitor error cause
- last reroute cause
- LSP monitor
- LSP path state and LSP path operating state
- LSP path type
- bypass tunnel active
- detour active
- MPLS path name and ID
- failure code

14

Click on the Segments tab button.

15

Click on the Search button and choose an entry.

16

Click on the Properties button. The Path Segment (Edit) form opens.

17

View the segment details.

18

Close the Path Segment (Edit) form.

19

Close the LSP Path Record (Edit) form.

20

Close the S2L Path Monitor (Edit) form.

21

Close the Path and Prefix Monitoring form.

END OF STEPS

8.20 To view historical path records of a monitored LSP path binding

8.20.1 Steps

1

Choose Manage→MPLS→LSP Path Optimization from the NFM-P main menu. The LSP Path Optimization form opens.

2

Choose LspPath (Path/Routing Management: MPLS) from the menu.

3

Specify a filter for the search, if required, and click on the Search button.

4

Choose an entry and click on the properties button. The LSP-Path Binding (Edit) form opens with the General tab displayed.

5

Click on the Navigate button and choose Historical Paths Records. The Path and Prefix Monitoring form opens.

6

Click on the Search button. A list of monitored paths appear.

Note: No entries appear if the path is not monitored. You can create a path monitor by performing 8.5 “To monitor a dynamic LSP” (p. 139) or 8.11 “To create an LSP path monitor from a dynamic LSP” (p. 150) .

7

Choose an entry and click on the Properties button. The LSP Path Record (Edit) form opens with the General tab displayed.

8

View the following information:

- record time
- monitor error cause
- last reroute cause
- LSP monitor
- LSP path state and LSP path operating state
- LSP path type
- bypass path active
- detour active
- MPLS path name and ID
- failure code

9

Click on the Segments tab button.

10

Click on the Search button and choose an entry.

11

Click on the Properties button. The Path Segment (Edit) form opens.

12

View the segment details.

13

Close the Path Segment (Edit) form.

14

Close the LSP Path Record (Edit) form.

15

Close the Path and Prefix Monitoring form.

16

Close the LSP Path-Binding (Edit) form.

17

Close the LSP Path Optimization form.

END OF STEPS

8.21 To view status change history of monitored prefixes

8.21.1 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

2

Choose Status change history (CPAM: Topology) from the object drop-down menu and click on the Search button. A list of prefixes appears.

3

Sort the list using the Status column menu. Choose one of the following:

- Added
- Does Not Exist
- Exists
- Next Hops Modified
- Removed
- Status Unknown

4

Choose an entry and click on the Properties button to view information about the prefix status change. The Status change history (Edit) form opens with the General tab displayed.

5

Close the Status change history (Edit) form.

6

Close the Path and Prefix Monitoring form.

END OF STEPS

8.22 To view the total cost of IP paths and IP path segments

8.22.1 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

2

Choose IP Path Record (Monitored Path) from the object menu and click on the Search button. A list of IP path records appears.

3

Choose an entry and click on the Properties button. The IP Path Record (Edit) form opens with the General tab displayed.

4

Click on the Total Cost tab button to view the total cost of the path.

5

Click on the Segments tab button. A list of path segments is displayed.

6

Choose an entry and click on the Properties tab button. The Segments (Edit) form opens.

Note: You can highlight a segment on the topology map by choosing an entry on the Segments tab button, and clicking on the Navigate button.

7

View the cost in the Link Cost panel.

8

Close the Segments (Edit) form.

9

Close the IP Path Record (Edit) form.

10

Close the Path and Prefix Monitoring form.

END OF STEPS

8.23 To navigate to a dynamic LSP on a topology map

8.23.1 Steps

1

Choose Manage→MPLS→Dynamic LSPs from the NFM-P main menu. The Manage Dynamic LSPs form appears.

2

Specify a filter for the search, if required, and click on the Search button. A list of dynamic LSPs appears.

3

Choose an entry and click on the Properties button. The Dynamic LSP (Edit) form opens with the General tab displayed.

4

Click on the Navigate button and choose one of the following options:

- IGP View
- ISIS View
- MPLS View
- OSPF View

5

Perform one of the following:

a. Choose Active Path→Active Path: IGP AD to highlight the active path on the topology map that you selected in Step 4 .

b. Choose Operational Paths→Operational Paths: IGP AD to highlight the operational paths on the topology map that you selected in Step 4 .

c. Choose Provisioned Path for the Active Path→Provisioned Path for the Active Path: IGP AD to highlight the provisioned path for the active path on the topology map that you selected in Step 4 .

d. Choose Provisioned Paths→Provisioned Paths: IGP AD to highlight the provisioned paths on the topology map that you selected in Step 4 .

e. Choose Show CSPF→Show CSPF: IGP AD to highlight the CSPF on the topology map that you selected in Step 4 . The Highlight CSPF form opens with the General tab displayed. Perform Step 3 to Step 13 of 7.11 “To highlight the constrained shortest path between two IP addresses” (p. 101) to create the CSPF highlight request.

6

Close the topology map.

7

Close the Dynamic LSP (Edit) form.

8

Close the Manage Dynamic LSP form.

END OF STEPS

8.24 To navigate to a monitored path on a topology map

8.24.1 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

2

Configure the list filter criteria and choose one of the following from the object menu.

- IP Path Record (Monitored Path)
- LSP Path Record (Monitored Path)

3

Specify a filter for the search, if required, and click on the Search button. A list of records appears.

4

Select a record and click on the Navigate button.

5

Choose a topology map view from the contextual menu.

6

The appropriate topology map opens with the highlighted path.

END OF STEPS

8.25 To find the cause event of an IP or LSP path record

8.25.1 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

2

Configure the list filter criteria and choose one of the following from the object menu:

- IP Path Record (Monitored Path)
- LSP Path Record (Monitored Path)

3

Click on the Search button. A list of records appears.

4

Select a record and click on the Navigate button.

5

Choose Mapping View : Find Cause Events : Display from the contextual menu. The Mapping View : Find Cause Events : Display form opens with the list of cause events.

6

Choose an entry and click on the Properties button. The appropriate properties form for the event opens with the General tab displayed:

- Router LSA (Edit)
- Network LSA (Edit)
- Link State PDU (Edit)
- Traffic Engineering Link TLV (Edit)

7

Depending on the event, different tab buttons appear. Click on the tab button to view information about the event.

8

Close the properties form.

9

Close the Path and Prefix Monitoring form.

END OF STEPS

8.26 To find the cause event of a path record of a service tunnel

8.26.1 Steps

1

Choose Manage→Service Tunnels from the NFM-P main menu. The Manage Service Tunnels form opens.

2

Specify a filter for the search, if required, and click on the Search button.

3

Select an entry and click on the Properties button. The Tunnel (Edit) form opens with the General tab displayed.

4

Click on the Navigate button and choose Historical Path Records from the contextual menu.

5

The Path and Prefix Monitoring form opens.

Note: If there is no IP path monitor associated with the service tunnel, the IP Path Monitor (Create) form opens with the General tab displayed. Perform Step 6 to Step 10 of 8.8 “To monitor an SDP tunnel” (p. 145) .

6

Click on the Search button. A list of path records appears.

7

Choose an entry and click on the Navigate button.

8

Choose Mapping View : Find Cause Events : Display from the contextual menu. The Mapping View : Find Cause Events : Display form opens with the list of cause events.

9

Choose an entry and click on the Properties button. The appropriate properties form for the event opens with the General tab displayed.

10

Depending on the event, different tab buttons appear. Click on the tab button to view information about the event.

11

Close the properties form.

12

Close the IP Path Monitor (Edit) form.

13

Close the Tunnel (Edit) form.

14

Close the Manage Service Tunnels form.

END OF STEPS

8.27 To find the IP or LSP path monitor record associated with a cause event

8.27.1 Steps

1

Choose Tools→Route Analysis→Historical Routing Events→IGP→LSAs from the NFM-P main menu. The LSAs form opens.

2

Choose IS-IS (Routing Management: ISIS) or OSPF (Routing Management: OSPF).

3

Perform one of the following:

a. For IS-IS events, click on Link State PDU (Routing Management: ISIS).

b. For OSPF events, expand LSA (Routing Management: OSPF) and click on one of the following:

- Network LSA (Routing Management: OSPF)
- Router LSA (Routing Management: OSPF)
- Traffic Engineering Link TLV (Routing Management: OSPF)

4

Click on the Search button. A list of events appears.

5

Select an event and click on the Properties button. Depending on the option you chose in Step 3 a or b , one of the following properties forms opens with the General tab displayed:

- Router LSA (Edit)
- Network LSA (Edit)
- Link State PDU (Edit)
- Traffic Engineering Link TLV (Edit)

6

Click on the Navigate button and choose Mapping View : Find Likely Re-Route : Display from the contextual menu. The Mapping View : Find Likely Re-Route : Display form opens. The search returns the records before and after the event that caused the reroute.

7

Choose an entry and click on the Properties button. The appropriate IP or LSP path record properties form.

8

Close the properties form.

9

Close the Historical Routing Events form.

END OF STEPS

8.28 To sort IP path records by error code

8.28.1 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

2

Configure the list filter criteria and choose IP Path Record (Monitored Path) from the object menu.

3

Click on the Search button. A list of IP path records appears.

4

Configure the filter criteria in the Error Code field.

1. Choose EQUALS or NOT EQUAL.
2. Choose an error code from the menu.

5

Click on the Search button. A list of entries that match the error code you selected in Step 4 appears.

6

Close the Path and Prefix Monitoring form.

END OF STEPS

8.29 To sort LSP path records by error code

8.29.1 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

2

Configure the list filter criteria and choose LSP Path Record (Monitored Path) from the object menu.

3

Click on the Search button. A list of LSP path records appears.

4

Configure the filter criteria in the Monitor Error Code field.

1. Choose EQUALS or NOT EQUAL.
2. Choose an error code from the menu.

5

Click on the Search button. A list of entries that match the error code you selected in Step 4 appears.

6

Close the Path and Prefix Monitoring form.

END OF STEPS

8.30 To sort LSP path records by last reroute cause

8.30.1 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

2

Configure the list filter criteria and choose LSP Path Record (Monitored Path) from the object menu.

3

Click on the Search button. A list of LSP path records appears.

4

Configure the filter criteria in the Last Reroute Cause field.

1. Choose EQUALS or NOT EQUAL.
2. Choose a last reroute cause from the menu.

5

Click on the Search button. A list of entries that match the last reroute cause you selected in Step 4 appears.

6

Close the Path and Prefix Monitoring form.

END OF STEPS

8.31 To delete historical events

8.31.1 Steps

1

Choose Tools→Route Analysis→Historical Routing Events→IGP from the NFM-P main menu. The Historical Routing Events form opens.

2

Depending on the object you want to delete, perform one of the following:

a. From the Filter menu, expand the IS-IS (Routing Management: ISIS) object and choose Link State PDU (Routing Management: ISIS).

b. From the Filter menu, expand the IS-IS (Routing Management: ISIS) object, expand the Neighbor TLV (Routing Management: ISIS) object, and choose IS Neighbor TLV (Routing Management: ISIS).

c. From the Filter menu, expand the IS-IS (Routing Management: ISIS) object, expand the Neighbor TLV (Routing Management: ISIS) object, and choose TE IS Neighbor TLV (Routing Management: ISIS).

d. From the Filter menu, expand the OSPF (Routing Management: OSPF) object, expand the LSA (Routing Management: OSPF) object, and choose Network LSA (Routing Management: OSPF).

e. From the Filter menu, expand the OSPF (Routing Management: OSPF) object, expand the LSA (Routing Management: OSPF) object, and choose Traffic Engineering Link TLV (Routing Management: OSPF).

f. From the Filter menu, expand the OSPF (Routing Management: OSPF) object and choose Link (Routing Management: OSPF).

3

Select one or more entries and click on the Delete button. A dialog box appears.

4

Click on the Yes button. The dialog box closes and the object is deleted.

5

Close the Historical Routing Events form.

END OF STEPS

9 Prefix lists

9.1 Prefix lists overview

9.1.1 Introduction

The CPAM retrieves advertised IGP or BGP prefixes from the CPAA. You can create and save filters to retrieve these prefixes, depending on the prefix type.

The prefixes that the CPAM retrieves from the CPAA are displayed with their related attributes. You can sort or filter the list of prefixes based on different route attributes.

9.2 Workflow for prefix lists

9.2.1 Stages

1

Create an IGP or BGP prefix list filter. See 9.3 “To create an IGP prefix list filter” (p. 177) and 9.5 “To create a BGP prefix list filter” (p. 179) for more information.

2

Retrieve the IGP or BGP filtered prefix list. See 9.4 “To retrieve a filtered IGP prefix list” (p. 178) and 9.6 “To retrieve a filtered BGP prefix list” (p. 182) for more information.

3

Cancel an ongoing retrieval, if required. See 9.7 “To cancel an ongoing retrieval” (p. 183) for more information.

9.3 To create an IGP prefix list filter

9.3.1 General information

Perform this procedure to create an IGP prefix list filter. To generate a filtered prefix list, see 9.4 “To retrieve a filtered IGP prefix list” (p. 178) .

Consider the following when you create an IGP prefix list:

- IGP prefix lists can be retrieved from only one administrative domain at a time
- You can filter IGP prefixes based on:
  - Protocol—OSPF, ISIS, or both
  - OSPF area
  - ISIS domain
  - ISIS instance
  - Prefix type (OSPF only)

- Advertising router
- Prefix range

9.3.2 Steps

1

Choose Tools→Route Analysis→Prefix List from the NFM-P main menu. The Prefix Form opens.

2

Click Create and choose IGP Prefix Filter. The IGP Prefix List Filter form opens.

3

Configure the required parameters.

Note: The OSPF Area Id parameter is configurable only if you enable the OSPF Area Id option in the Prefix Filters panel.
The Prefix Lower Range and Prefix Higher Range parameters are configurable only if you enable the Prefix Range option in the Prefix Filters panel.
The CPAA Address parameter is configurable only if you enable the CPAA Address option in the Prefix Filters panel and the Protocol parameter is set to ISIS or OSPF/ISIS.
The CPAA Instance ID parameter is configurable only if you enable the CPAA Address option in the Prefix Filters panel.
The Advertising Router parameter is configurable only if you enable the Advertising Router option in the Prefix Filters panel.
The Prefix Type parameter is configurable only if the Protocol parameter is set to OSPF or OSPF/ISIS.
The ISIS Domain parameter is configurable only if the Protocol parameter is set to ISIS or OSPF/ISIS.

4

Save the configuration and close the IGP Prefix List Filter form.

END OF STEPS

9.4 To retrieve a filtered IGP prefix list

WARNING

Equipment Damage

Generating a filtered prefix list may impact performance of the CPAM, depending on the size of the network.

Note: It can take up to 10 minutes to retrieve a filtered prefix list. During this time, no other retrievals can be performed. A warning message appears if another user attempts to perform

a retrieval during this time. Any user can cancel the retrieval process. See 9.7 “To cancel an ongoing retrieval” (p. 183) for information.

9.4.1 Steps

1

Choose Tools→Route Analysis→Prefix List from the NFM-P main menu. The Prefix Form opens.

2

Choose IGP Prefix List Filter and click Search. A list of prefix list filters appears.

3

Choose a prefix list filter and click Properties. The IGP Prefix List Filter form opens.

4

Click Retrieve IGP Prefix and choose the IGP administrative domain on which you want to generate the prefix list from the contextual menu.

5

Click on the IGP Prefix Retrieval tab and click Search. A list of retrieved IGP prefixes appears.

6

Choose a retrieved IGP prefix and click Properties. The Retrieved IGP Prefixes form opens.

7

Click on the IGP Prefix Info tab and click Search. A list of IGP prefixes appears.

8

Choose an IGP prefix and click Properties. The IGP Prefix form opens.

9

Review the information and close the IGP Prefix form.

10

Save your changes and close the forms.

END OF STEPS

9.5 To create a BGP prefix list filter

9.5.1 General information

Perform this procedure to create a BGP prefix list filter. To generate a filtered prefix list, see 9.6 “To

retrieve a filtered BGP prefix list" (p. 182) .

Consider the following when you create a BGP prefix list:

- BGP prefix lists can be retrieved from only one AS at a time
- You can filter BGP prefixes based on:
  - protocol—IPv4 or VPN IPv4
  - EVPN
  - RT (VPN IPv4 only)
  - route distinguisher (VPN IPv4 only)
  - prefix health (VPN IPv4 only)
  - originating AS
  - MED
  - local preference
  - next hop
  - route type—internal, external, or both
  - AS path length

9.5.2 Steps

1

Choose Tools→Route Analysis→Prefix List from the NFM-P main menu. The Prefix Form opens.

2

Click Create and choose BGP Prefix Filter. The BGP Prefix List Filter form opens.

3

Configure the required parameters.

Note: When you choose EVPN as the address type, the EVPN Route Type panel is available.
The Prefix Lower Range and Prefix Higher Range parameters are configurable only if you enable the Prefix Range option in the Prefix Filters panel.
The Local Preference parameter is configurable only if you enable the Local Preference option in the Prefix Filters panel.
The Min. Health Indicator %, Max. Health Indicator % , Duration, and Duration Unit parameters are configurable only if you enable the Health Indicator option in the Prefix Filters panel, and if the Local Preference, MED, Path Length, and Route Target options are disabled. The Health Indicator option can be enabled for IPv4, VPN IPv4, IPv6, and VPN IPv6 BGP prefixes.
The Originating AS parameter is configurable only if you enable the Originating AS option in the Prefix Filters panel.
The Prefix Type parameter is configurable only if you enable the Prefix Type option in the Prefix Filters panel.

The Next Hop parameter is configurable only if you enable the Next Hop option in the Prefix Filters panel.
The Route Distinguisher Type and Route Distinguisher parameters are configurable only if you enable the Route Distinguisher option in the Prefix Filters panel.
The MED parameter is configurable only if you enable the MED option in the Prefix Filters panel.
The AS Path Length parameter is configurable only if you enable the Path Length option in the Prefix Filters panel.
The Type and Route Target parameters are configurable only if you enable the Route Target option in the Prefix Filters panel.

Note: The Health Indicator option identifies the percentage of time that a prefix has been seen by the BGP for the last few days. The health indicator identifies how stable a prefix is. The health indicator is configured as a percentage from 0% to 100%, for a number of days, from 1 to 7. For example, if you set the health indicator to 90% for the last 3 days, all of the prefixes that have been available for at least 90% of the time during last 3 days are retrieved. When you select only the Health Indicator option, the retrieved prefix list does not contain any route attributes, such as Next Hop or MED.
The CPAA keeps track of all of the VPN IPv4 MP-BGP prefixes for up to 7 days, and calculates how long the prefix has been available. The prefix availability time is aggregated and stored every hour for 24 hours and every day for 7 days. When the BGP is activated on the CPAA, it starts its internal hourly and daily timer to aggregate the prefix availability time. For instance, if BGP comes up at 3:25 AM on the CPAA clock, the CPAA performs the aggregation every hour at the 25 minutes past the hour and every day at 3:25 AM. The CPAA keeps the results of last 24 hourly and 7 daily aggregations. If a user at 10 AM tries to retrieve all of the prefixes that have been available for last day, the prefixes that have a health indicator of 100% for the last 6 hours and 35 minutes—the time since 3:25 AM—are retrieved. To prevent confusion on the BGP Prefix Info tab of the Retrieved BGP Prefixes (Edit) form, the exact duration for the health indicator calculation, (6 hours and 30 minutes in this example), and the start of the 24 hours aggregation period, (3:25 AM in this example), are reported.
The CPAM displays the status of the prefix—present or deleted—for the retrieved prefix health on the BGP Prefix Info tab for the retrieved prefixes. For absent prefixes, the down time since the deletion is displayed.

4

Perform the following if you enabled the Community Strings option in the Prefix Filters panel:

1. Click on the Communities tab and click Add.
2. Configure the Value parameter and click OK.

5

Save your changes and close the BGP Prefix List Filter form.

END OF STEPS

9.6 To retrieve a filtered BGP prefix list

WARNING

Equipment Damage

Generating a filtered prefix list may impact performance of the CPAM, depending on the size of the network.

Note: It can take up to 10 minutes to retrieve a filtered prefix list. During this time, no other retrievals can be performed. A warning message appears if another user attempts to perform a retrieval during this time. Any user can cancel the retrieval process. See 9.7 “To cancel an ongoing retrieval” (p. 183) for information.

9.6.1 Steps

1

Choose Tools→Route Analysis→Prefix List from the NFM-P main menu. The Prefix Form opens.

2

Choose BGP Prefix List Filter (CPAM:Topology) and click Search. A list of prefix list filters appears.

3

Choose a prefix list filter and click Properties. The BGP Prefix List Filter form opens.

4

Click Retrieve BGP Prefix and choose the AS or sub-AS on which you want to generate the prefix list from the contextual menu.

5

Close the BGP Prefix List Filter form.

6

Click on the BGP Prefix Retrieval tab and click Search. A list of retrieved BGP prefixes appears.

7

Choose a retrieved BGP prefix and click Properties. The Retrieved BGP Prefixes form opens.

8

Click on the BGP Prefix Info tab and click Search. A list of BGP prefixes appears.

9

Choose a BGP prefix and click Properties. The BGP Prefix form opens.

10

Review the information and close the BGP Prefix form.

11

Click on the BGP AS-PATH tab and click Search. A list of BGP AS paths appears.

12

Choose a BGP AS path and click Properties. The BGP AS-Path form opens.

13

Review the information and close the BGP AS-Path form.

14

Save your changes and close the forms.

END OF STEPS

9.7 To cancel an ongoing retrieval

9.7.1 Steps

1

Choose Tools→Route Analysis→Prefix List from the NFM-P main menu. The Prefix Form opens.

2

Perform one of the following:

a. Choose IGP Prefix List and click Search. A list of IGP prefix lists appears.

b. Choose BGP Prefix List and click Search. A list of BGP prefix lists appears.

3

Choose the prefix list for which you want to cancel the retrieval and click Properties. The *IGP/BGP* Prefix List form opens.

4

Verify the Retrieval Status. If the Retrieval Status is In Progress or Session Locked, click Abort to cancel the retrieval operation. The Retrieval Status is Aborted.

5

Save your changes and close the forms.

END OF STEPS

Part IV: BGP

Overview

Purpose

This volume provides information about BGP.

Contents

10 BGP management

10.1 BGP overview

10.1.1 Introduction

BGP is an inter-AS routing protocol. BGP allows devices to exchange network reachability information. The two types of BGP are:

- IBGP—to communicate with peer devices in the same AS. Routes received from a device in the same AS are not advertised to other devices in the same AS but can be advertised to an EBGP peer.
- EBGP—to communicate with peers in different ASs. Routes received from a device in another AS can be advertised to EBGP and IBGP peers.

See “BGP” in the *NSP NFM-P Classic Management User Guide* for information about how to configure BGP using the NFM-P. See the appropriate device documentation for information about router-specific BGP configurations.

10.1.2 BGP and CPAM

The CPAM extracts BGP route information from the BGP RIB that is maintained by a CPAA.

Network and element management systems, such as the NFM-P, can be used to configure BGP on devices and perform the following functions:

- set the AS values for the routing instance
- create confederations of group-managed devices
- create BGP peer groups
- create peers within the BGP peer groups
- retrieve statistical information
- monitor BGP-related network events

BGP routing information is not typically monitored by these systems because of the high volume of BGP and MP-BGP routes,

The CPAM discovers and monitors BGP routing information by consolidating the data from the CPAAs and providing an overview of a carrier network. You can use the information to, for example, monitor whether the change in the number of BGP routes may compromise the stability of the network, or if key BGP routes are disappearing. For VPRN routes, a high rate of change for a set of VRFs is flagged by the CPAM.

Note: The number of routes sent out for an RT from a PE is captured by the CPAA MP-BGP. The CPAM displays the number of routes and exported routes for a VRF.

The CPAM and the CPAA use peering sessions, originator IDs and next hops in the advertised routes to detect BGP speakers. The CPAM is aware of the NFM-P-managed routers that are running BGP.

10.1.3 BGP and the CPAA

You can specify the role of a CPAA: IGP, BGP, or both. The role of the CPAA indicates to the CPAM whether information from a protocol should be interpreted. A CPAA with an IGP role must be assigned to an IGP administrative domain. A CPAA with a BGP role must be assigned to a BGP AS. See 10.1.4 “CPAM administrative domains” (p. 187) for information.

The CPAA monitors a BGP AS and maintains a BGP RIB that is used by the CPAM to extract BGP route information. The CPAA supports the following BGP configurations:

- BGP AS
- BGP confederation AS
- BGP sub-AS

The CPAA does not send route updates to its peers or forward data traffic. The CPAA maintains a route table for all of the known routes. The CPAA should not function as a route reflector. In addition, EBGP peering is blocked. BGP is restricted to the core routing instance because services cannot be configured on the CPAA.

The CPAA should be peered with all of the route reflectors or with all of the IBGP speakers (full mesh topology) of the BGP AS or BGP sub-AS. See 10.2 “BGP topologies in CPAM” (p. 191) for information about the deployment of the CPAA in supported topologies.

Note: Nokia recommends that the CPAA establish an IBGP connection with the BGP speakers, not the route reflector, because the route reflector advertises only one preferred next-hop.

10.1.4 CPAM administrative domains

WARNING

Equipment Damage

The IGP administrative domain should generally be public IP address spaces, not private IP address spaces. If two IGP administrative domains have duplicate router IDs, for example, some functionality—such as the IP path monitor and managed routes—may not work correctly.

An administrative domain is a user-configured grouping that represents a logical routed network. The CPAM supports the following administrative domains:

- **IGP administrative domain**
  A routed network with OSPF, ISIS, or both protocols running. There can be only one backbone domain for each protocol. For OSPF, multiple areas with the same area ID cannot exist.
- **BGP AS**
  An administrative domain which represents the standard BGP AS, confederation AS, or sub-AS. A BGP confederation AS administrative domain contains other BGP sub-ASs.

An IGP administrative domain is uniquely identified by a domain number and name that are configured when it is created. A CPAA that is configured with an IGP role must be assigned to an IGP administrative domain. Each CPAA can be assigned to only one IGP administrative domain. A BGP AS is identified by a BGP AS number, which should be identical to the network-configured

BGP AS, a BGP AS name, and BGP AS type. Each BGP AS administrative domain is associated with only one IGP administrative domain. An IGP administrative domain can be associated with several BGP AS administrative domains. A CPAA that is configured with a BGP role must be assigned to each BGP AS administrative domain. Each CPAA can be assigned to only one BGP AS administrative domain.

The BGP AS administrative domain in the CPAM models the actual BGP AS that is being monitored by a CPAA with a BGP role. One CPAA is used to monitor BGP routes in each AS or sub-AS, that is associated with an IGP administrative domain in the CPAM. The following types of BGP AS are monitored:

- standard BGP AS
- BGP sub-AS (within a confederation AS)

A standard BGP AS uses a registered BGP AS identifier to advertise its known BGP routes to other registered AS domains.

A BGP sub-AS can exist within a confederation AS administrative domain and uses a private AS identifier to advertise routes to other BGP sub-AS domains within the registered AS. The use of sub-AS domains reduces the number of IBGP sessions between routers and the number of BGP routes advertised between registered AS domains. Confederations do not reduce the number of updates between the ASs.

BGP sub-AS administrative domains are created in the CPAM within a confederation AS. A standard AS uses a CPAA to monitor the entire AS. For BGP confederation AS domains, each sub-AS domain should be monitored using a different CPAA.

10.1.5 MP-BGP

The CPAA collects MP-BGP routing information when the VPN IPv4 address family is activated on each IBGP peering session. The CPAA uses the RT of the advertised routes to differentiate between the VPN sites. Although a VPN site can be assigned more than one RT, the CPAA cannot make this association from the routing updates. The next hops in the advertised routes identify the PEs for the specific RT.

You can use the CPAM to retrieve MP-BGP information, such as the number of routes per RT. In addition, you can retrieve the list of next hops and number of routes per next hop for each RT. The CPAA monitors the number of routes for each RT and, if you configure threshold reaching alarms, raises alarms when the number of routes reaches the configured threshold, such as low water mark, high water mark, and flap rate.

10.1.6 BGP RIB information

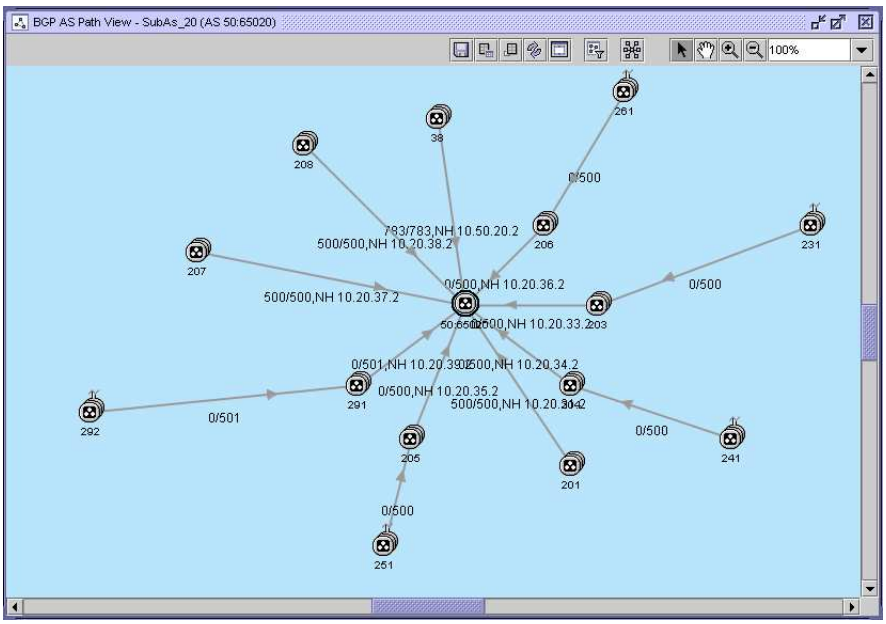
You can use the CPAM to view BGP attribute information about BGP advertised prefixes. The CPAA collects the following BGP RIB information, that can be viewed in the CPAM:

- routes with the same advertised BGP next hop
- routes that share the same route reflector originator ID (originator of the route into the AS)
- routes with the same MED
- IBGP routes with the same local preference attribute
- routes with the same BGP communities attribute

10.1.7 BGP AS path view

The BGP AS path view is an on-demand graphical representation of the entire BGP network from the perspective of a BGP AS or sub-AS, as displayed in the figure below. Because only one CPAA can be associated with a BGP AS, the BGP AS path view displays the BGP network from the perspective of one CPAA. A BGP AS or sub-AS is represented as a node on the topology map.

Figure 10-1 BGP AS path view



Each arrow represents at least one EBGP connection between two BGP ASs or sub-ASs and indicates the direction of EBGP update message from the originating AS to the terminating AS. Each link on the map displays the number of EBGP routes that are advertised from one AS to another AS, in the direction indicated by the arrow.

You can specify the number of ASs and next hops that are displayed on the map, as described in 10.16 “To view BGP AS path topology” (p. 210) .

You can view the information displayed on the BGP AS path view from the ASN and ASN link forms. See 10.11 “To view ASN link information” (p. 203) to 10.16 “To view BGP AS path topology” (p. 210) for information.

10.1.8 BGP highlighting

You can use the CPAM to highlight all of the NEs that advertise a prefix into an AS on the IGP topology map. You must specify a BGP prefix, and an RD for VPN IPv4 prefixes. The CPAM highlights all of the NEs that advertise a route for that prefix into the administrative domain. The router or routers which advertise the preferred route, based on the BGP attributes, are highlighted in a different color from the other advertising routers. See 10.22 “To highlight advertising routers for

BGP prefixes" (p. 191) for information about how to configure the highlighting of advertising routers that advertise prefixes into an AS or sub-AS.

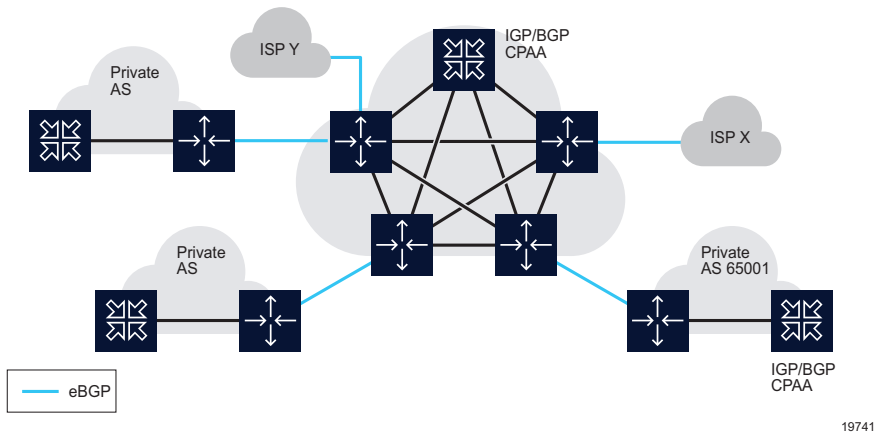
10.2 BGP topologies in CPAM

10.2.1 BGP AS with meshed IBGP connections

In this topology, EBGP is used between ASs and a full mesh IBGP is created within each AS, as displayed in Figure 10-2, "BGP AS with meshed IBGP connections sample topology" (p. 190) . The BGP CPAA also has a full IBGP connection to all other BGP speakers in the AS. An IGP administrative domain—an instance of OSPF, ISIS, or both routing protocols—is used in the BGP AS for reachability between routes in the AS and for BGP next hop resolution.

In this case, you use the CPAM to create a BGP AS and an IGP administrative domain for each AS that is managed by the service provider. The BGP AS is assigned the appropriate IGP administrative domain. You can specify a CPAA with both IGP and BGP roles and assign the CPAA to the BGP AS and IGP administrative domains. You can also assign another CPAA to each administrative domain—IGP and BGP.

Figure 10-2 BGP AS with meshed IBGP connections sample topology



10.2.2 Private AS with no confederation

From the perspective of the CPAM, the management of this network is the same as a network with multiple registered ASs, as displayed in Figure 10-2, "BGP AS with meshed IBGP connections sample topology" (p. 191) . A different IGP administrative domain is associated with each private AS. A BGP CPAA must be assigned to each BGP AS.

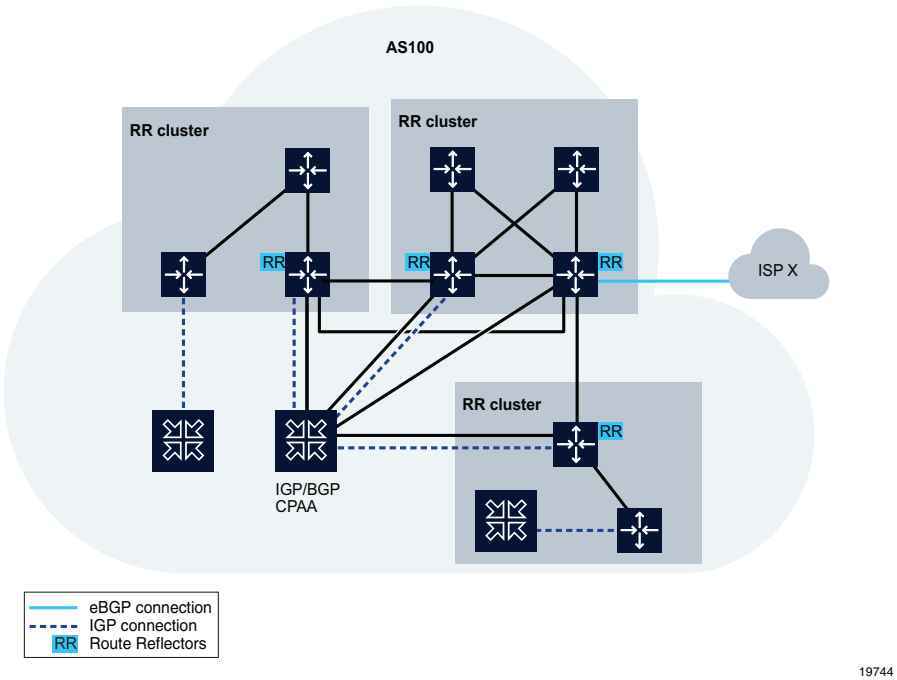
In this case, you use the CPAM to create a BGP AS and an IGP administrative domain for each private AS managed by the provider. The BGP AS is assigned the appropriate IGP administrative domain. You can specify a CPAA with both IGP and BGP roles and assign the CPAA to the BGP AS and IGP administrative domains. You can also assign a different CPAA to each administrative domain, that is, IGP and BGP.

10.2.3 AS with route reflectors

The route reflector topology is an alternative to the IBGP full mesh within an AS, when numerous IBGP speakers exchange a large volume of routing information. BGP speakers, or route reflectors, can then advertise IBGP learned routes to IBGP peers. Figure 10-3, “AS with route reflectors sample topology” (p. 191) shows an AS with four route reflectors. A route reflector along with its client peers forms a cluster. The route reflector redistributes routing updates to all of the devices in the cluster. Because the route reflector provides all of the routing updates, the other devices in the cluster do not maintain a BGP mesh.

You must assign one BGP CPAA to each AS. The CPAA needs a full mesh of IBGP non-client peering sessions to all of the route reflectors and all of the non-client routers. IGP is used for reachability between BGP routers in an AS.

Figure 10-3 AS with route reflectors sample topology



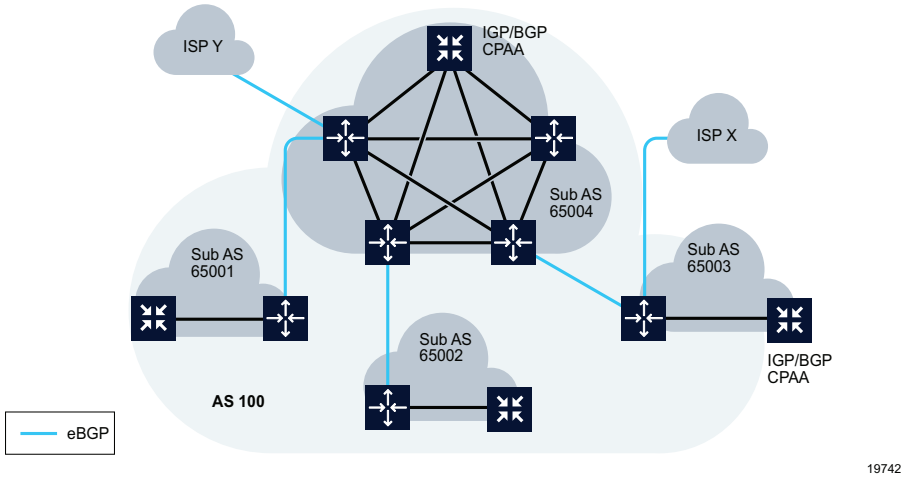
10.2.4 BGP confederation AS with one IGP administrative domain in each sub-AS

This topology is an alternative to the route reflector topology and alleviates the requirement for an IBGP full mesh. The confederation AS is divided into smaller ASs called sub-ASs, as displayed in Figure 10-4, “BGP confederation AS with one IGP administrative domain in each sub-AS sample topology” (p. 193) . A full mesh of IBGP connectivity exists within each sub-AS. The sub-ASs are connected to each other using the EBGP peering session. Each sub-AS is assigned a private AS number that is only visible within the AS. Sub-ASs are hidden from all of the BGP routers outside the AS. Sub-ASs are visible only inside the confederation AS.

Each sub-AS is monitored by one BGP CPAA. There is a full mesh of IBGP connectivity between the BGP CPAA and all of the other BGP routers within a sub-AS. One IGP protocol is configured in each sub-AS.

In this topology, a BGP sub-AS administrative domain is configured for each sub-AS and a separate IGP administrative domain is created and assigned to each sub-AS.

Figure 10-4 BGP confederation AS with one IGP administrative domain in each sub-AS sample topology



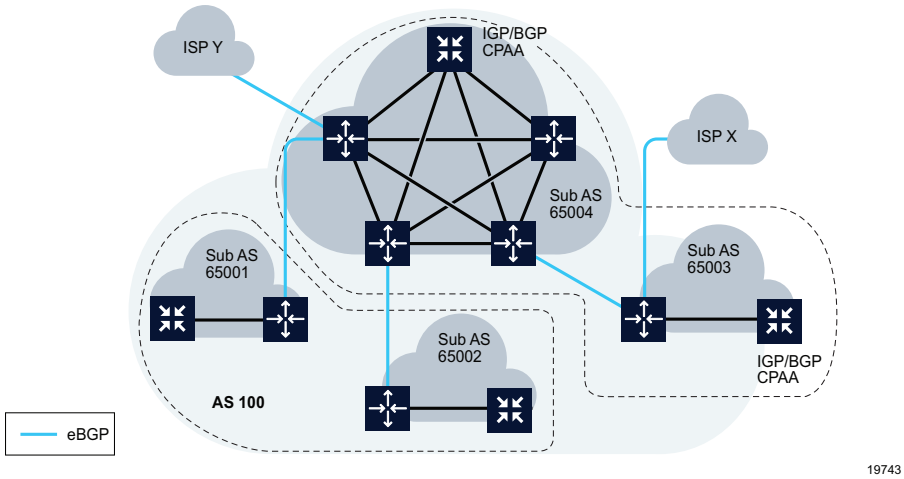
10.2.5 BGP confederation AS with one IGP administrative domain

This topology is similar to the topology described in 10.2.4 “BGP confederation AS with one IGP administrative domain in each sub-AS” (p. 192) . Only one IGP administrative domain is assigned to the entire confederation AS. Each sub-AS is assigned to the same IGP administrative domain.

10.2.6 BGP confederation AS with multiple IGP administrative domains

In this topology, multiple BGP sub-AS administrative domains share one of several IGP administrative domains, as displayed in the figure below. One BGP CPAA is assigned to each sub-AS within the confederation and can also be used to support all or part of the associated IGP administrative domain. In addition, one or more CPAAs can be used for each IGP administrative domain in the IGP topology. If multiple sub-ASs share an IGP administrative domain, only one of the BGP CPAAs can monitor the shared IGP administrative domain. The other BGP CPAAs cannot monitor the IGP administrative domain.

Figure 10-5 BGP confederation AS with multiple IGP administrative domains sample topology



10.3 Workflow for BGP management

10.3.1 Stages

1

Identify logical IGP networks and create an IGP administrative domain for each. See 10.4 “To configure an IGP administrative domain” (p. 196) for more information.

2

Identify all of the BGP AS domains that do not contain sub-AS domains and create a BGP AS administrative domain, using the standard BGP AS type for each. Assign the corresponding IGP administrative domain to each BGP AS administrative domain and deploy a dedicated CPAA to monitor the BGP AS. See 10.5 “To create a BGP standard AS” (p. 196) for more information.

3

Identify all of the BGP confederation AS domains that contain sub-AS domains and create a BGP AS administrative domain using the confederation AS type. Create a BGP sub-AS administrative domain for each sub-AS within the confederation BGP AS administrative domain. For each BGP sub-AS, assign the corresponding IGP administrative domain to the BGP AS administrative domain and deploy a dedicated CPAA to monitor the BGP AS. See 10.6 “To create a BGP confederation AS” (p. 197) and 10.7 “To add a BGP sub-AS to a confederation AS” (p. 198) for more information.

4

Configure each BGP CPAA to monitor BGP AS administrative domains. See 10.8 “To deploy a CPAA to monitor a BGP AS” (p. 199) for more information.

5

Retrieve BGP AS information from the CPAA. See 10.9 “To retrieve BGP information from a CPAA” (p. 201) for more information.

6

View retrieved BGP AS and CPAA information, as required.

- View discovered ASN information. See 10.10 “To view discovered ASN information” (p. 202) for more information.
- View ASN link information. See 10.11 “To view ASN link information” (p. 203) for more information.
- View BGP RIB information. See 10.12 “To view BGP RIB information” (p. 204) for more information.
- View RT retrieval information. See 10.13 “To view RT retrieval information” (p. 205) for more information.
- View IP VPN route targets. See 10.14 “To view IP VPN route targets” (p. 207) for more information.
- View L2 VPN route targets. See 10.15 “To view L2-VPN route targets” (p. 209) for more information.
- View BGP AS path topology. See 10.16 “To view BGP AS path topology” (p. 210) for more information.
- View corrupted BGP update records. See 10.17 “To view corrupted BGP update records” (p. 213) for more information.
- View CPAA update times information. See 10.18 “To view CPAA update times information” (p. 214) for more information.
- View BGP routes and paths. See 10.19 “To view BGP routes” (p. 214) and 10.20 “To view BGP paths” (p. 215) for more information.

7

Navigate to VPN IPv4 or L2 VPN route targets on a topology map. See 10.21 “To navigate to PE routers advertising an RT on a topology map” (p. 216) for more information.

8

Highlight all of the NEs that advertise a prefix into the AS or sub-AS, if required. See 10.22 “To highlight advertising routers for BGP prefixes” (p. 217) for more information.

9

Configure BGP-monitoring threshold reaching alarms. See 16.3 “To configure alarm thresholds” (p. 295) in Chapter 16, “Threshold reaching alarms” for more information.

10.4 To configure an IGP administrative domain

10.4.1 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.

2

Click on the Create button and choose Create IGP Admin Domain from the contextual menu. The IGP Administrative Domain (Create) form opens with the General tab displayed.

3

Configure the parameters:

- IGP Admin Domain Name
- IGP Admin Domain Number
- Description

Note: To avoid upgrade problems, ensure that the IGP Admin Domain Number parameter is correctly configured.

4

Configure the Enabled Menus parameter.

5

Click on the OK button to save the configuration and close the form.

END OF STEPS

10.5 To create a BGP standard AS

10.5.1 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.

2

Click on the Create button and choose Create BGP AS from the contextual menu. The BGP Autonomous System, AS (Create) form opens with the General tab displayed.

3

Set the Type parameter to AS.

4

Configure the parameters:

- AS Number
- AS Name
- Description
- Depth Value for Retrieve AS Path

5

Click on the Select button next to the IGP Admin Domain Number parameter. The Select IGP Administrative Domain - BGP Autonomous System - AS form opens.

6

Choose an entry and click on the OK button. The Select IGP Administrative Domain - BGP Autonomous System - AS form closes and the BGP Autonomous System - AS (Create) form refreshes with the IGP administrative domain information.

7

To configure monitored prefixes, perform 8.15 “To configure BGP monitored prefixes” (p. 157) .

8

Click on the OK button. The BGP Autonomous System, AS (Create) form closes.

9

Close the Admin Domains / CPAAs form.

END OF STEPS

10.6 To create a BGP confederation AS

10.6.1 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.

2

Click on the Create button and choose Create BGP AS from the contextual menu. The BGP Autonomous System, AS (Create) form opens with the General tab displayed.

3

Set the Type parameter to Confederation AS.

4

Configure the parameters:

- AS Number
- AS Name
- Description

5

Perform 10.7 “To add a BGP sub-AS to a confederation AS” (p. 197) to add one or more sub-ASs to the confederation AS.

6

Close the Admin Domains / CPAAs form.

END OF STEPS

10.7 To add a BGP sub-AS to a confederation AS

10.7.1 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.

2

Choose and expand the Administrative Domain (CPAM: Topology) object in the object drop-down menu.

3

Click on the BGP Autonomous System (CPAM: Topology) object.

4

Specify a filter to search for BGP confederation AS types and click on the Search button. A list of configured BGP ASs appears.

5

Choose a BGP confederation AS and click on the Properties button. The BGP Autonomous System - Confederation AS (Edit) form opens with the General tab displayed.

6

Click on the BGP Sub-AS tab.

7

Click on the Add button. The BGP Autonomous System, Sub-AS (Create) form opens with the General tab displayed.

8

Configure the parameters:

- AS Number
- AS Name
- Description
- Depth Value for Retrieve AS Path

9

Click on the Select button next to the IGP Admin Domain Number parameter. The Select IGP Administrative Domain - BGP Autonomous System - Sub-AS form opens.

10

Choose an entry and click on the OK button. The Select IGP Administrative Domain - BGP Autonomous System - Sub-AS form closes and the BGP Autonomous System - Sub-AS (Create) form refreshes with the IGP administrative domain information.

11

Click on the OK button. A dialog box appears.

12

Click on the OK button. The BGP Autonomous System, Sub-AS (Create) form closes.

13

Click on the OK button. A dialog box appears.

14

Click on the Yes button. The BGP Autonomous System, Confederation AS (Edit) form closes.

END OF STEPS

10.8 To deploy a CPAA to monitor a BGP AS

10.8.1 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.

2

Choose CPAA (CPAM: Topology) from the object drop-down menu and click on the Search button. A list of discovered CPAAs appears.

3

Configure each CPAA by performing the following:

1. Double-click on an entry in the list of discovered CPAAs. The CPAA (Edit) form opens with the General tab displayed.
2. Set the Administrative State parameter to Down.

   Note:

   Nokia recommends that you apply a reference to the CPAA before you make any configuration changes.

   Alternatively, you can view and configure the route listening and analysis parameters from the CPAA tab of the CPAA Network Element (Edit) form. Right-click on a CPAA in the equipment view of the navigation tree and choose Properties from the contextual menu. Click on the CPAA Properties button.

   See the *7701 CPAA Setup and Installation Guide* for information about how to configure a CPAA to monitor an IGP administrative domain.

4

Click on the Administrative Domains tab.

5

Configure the Role parameter. You must enable the BGP option.

Note: To remove a role from a CPAA that is assigned to an administrative domain, set the Administrative State parameter to Down, remove the role, and click on the Apply button. The CPAM automatically removes the selected administrative domain.

6

Associate the CPAA with a BGP AS by clicking on the Select button next to the Type parameter.

The Select BGP AS/Sub-AS - CPAA form opens with a list of configured BGP AS.

7

Click on the General tab.

8

Set the Administrative State parameter to Up.

9

Click on the Apply button. The area topology is sent to the CPAM from the CPAA.

10

Close the Admin Domains / CPAAs form.

END OF STEPS

10.9 To retrieve BGP information from a CPAA

10.9.1 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.

2

Choose CPAA (CPAM: Topology) from the object drop-down menu and click on the Search button. A list of discovered CPAAs appears.

3

Select a CPAA and click on the Properties button. The CPAA (Edit) form opens with the General tab displayed.

4

Click on the Retrieve from CPAA button. If the Retrieve from CPAA is not visible, click on the More Actions button and choose Retrieve from CPAA. Choose one of the following:

- BGP AS Path Data
- BGP RIB Info
- IP VPN Route Targets
- L2-VPN Route Targets

A dialog box appears.

Note: Alternatively, you can retrieve BGP information from a CPAA on the BGP Network Data form. Choose Tools→Route Analysis→ BGP Network Data from the NFM-P main menu. Click on the Retrieve BGP Data and choose one of the following:

- BGP AS Path Data
- BGP RIB Info
- IP VPN Route Targets
- L2-VPN Route Targets
  A dialog box appears.

5

Click on the Yes button. The dialog box closes.

6

Close the Admin Domains / CPAAs form.

7

Perform 10.10 “To view discovered ASN information” (p. 201) to 10.15 “To view L2-VPN route targets” (p. 209) to view the retrieved data.

END OF STEPS

10.10 To view discovered ASN information

10.10.1 Steps

1

Perform 10.9 “To retrieve BGP information from a CPAA” (p. 201) to retrieve BGP AS information from a CPAA.

2

Choose Tools→Route Analysis→BGP Network Data from the NFM-P main menu. The BGP Network Data form opens.

3

Choose ASN (CPAM: Topology) from the object drop-down menu and click on the Search button. A list of discovered ASNs appears.

4

Choose an entry and click on the Properties button. The ASN (Edit) form opens.

5

View the following information:

- discovered AS number
- BGP CPAA that discovered the AS
- confederation BGP AS number that discovered the AS, if applicable
- segment type:
  - SET — unordered set of ASs that a route in the UPDATE message has traversed
  - SEQUENCE — ordered set of ASs that a route in the UPDATE message has traversed
  - CONF-SEQ — ordered set of member-AS numbers in the confederation that the UPDATE message has traversed
  - CONF-SET — unordered set of member-AS numbers in the confederation that the UPDATE message has traversed
- indicator of whether the value configured for the Depth Value for Retrieve AS Path parameter has been met

- number BGP routes that originate from the AS
- number of hops away from the BGP CPAA

6

Close the ASN (Edit) form.

7

Close the BGP Network Data form.

END OF STEPS

10.11 To view ASN link information

10.11.1 Steps

1

Perform 10.9 “To retrieve BGP information from a CPAA” (p. 201) to retrieve BGP AS information from a CPAA.

2

Choose Tools→Route Analysis→BGP Network Data from the NFM-P main menu. The BGP Network Data form opens.

3

Choose ASN Link (CPAM: Topology) from the object drop-down menu and click on the Search button. A list of discovered ASNs appears.

4

Choose an entry and click on the Properties button. The ASN Link (Edit) form opens.

5

View the following ASN link information:

- AS numbers of the originating AS and terminating AS
- BGP CPAA that discovered the AS
- confederation BGP AS number that discovered the AS, if applicable
- next hop, if the AS is one hop away from the BGP CPAA
- number BGP routes that originate from the AS
- number of hops away from the BGP CPAA

6

Close the ASN Link (Edit) form.

7

Close the BGP Network Data form.

END OF STEPS

10.12 To view BGP RIB information

10.12.1 Steps

1

Perform 10.9 “To retrieve BGP information from a CPAA” (p. 201) to retrieve BGP AS information from a CPAA.

2

Choose Tools→Route Analysis→BGP Network Data from the NFM-P main menu. The BGP Network Data form opens.

3

Choose BGP RIB Info (CPAM: Topology) from the object drop-down menu and click on the Search button. A list of BGP RIB information entries appears, including entries for the following RIB attributes:.

- **NextHop**
  the next hop in the AS path to the destination
- **MED**
  The multi-exit discriminator metric that is used to differentiate between multiple exit points to the same peer AS
- **LOCAL-PREF**
  An attribute communicated to IBGP peers that is used to set preferences among multiple routes to the same destination.
- **ORIGINATOR-ID**
  ID of the router that originated the route into the AS
- **PEER**
  BGP peer information

4

Choose an entry and click on the Properties button. The appropriate properties form opens with the following information:

- **NextHop**
  - timestamp of retrieval
  - BGP AS number
  - IP address of next hop
  - number of routes exchanged

- **MED**
  - timestamp of retrieval
  - BGP AS number
  - MED value — a lower value is preferred
  - number of routes
- **LOCAL-PREF**
  - timestamp of retrieval
  - BGP AS number
  - LOCAL-PREF value — a higher value is preferred
- **ORIGINATOR-ID**
  - timestamp of retrieval
  - BGP AS number
  - ID of router from which routes originate
  - number of routes from originating router
- **PEER**
  - timestamp of retrieval
  - BGP AS number
  - peer IP address
  - number of routes exchanged

5

Close the properties form.

6

Close the BGP Network Data form.

END OF STEPS

10.13 To view RT retrieval information

10.13.1 Steps

1

Perform 10.9 “To retrieve BGP information from a CPAA” (p. 201) to retrieve BGP AS information from a CPAA.

2

Choose Tools→Route Analysis→BGP Network Data from the NFM-P main menu. The BGP Network Data form opens.

3

Choose Route Target Retrieval Record (CPAM: Topology) from the object drop-down menu and click on the Search button. A list of timestamped RT retrieval record entries appears.

4

Choose an entry and click on the Properties button. The Route Target Retrieval Record (Edit) form appears with the General tab displayed.

5

View the following information:

- timestamp of retrieval
- BGP AS number
- BGP confederation AS number, if applicable

6

Perform one of the following:

a. If you chose a VPN IPv4 RT retrieval record, click on the IP VPN Route Target tab. A list of VPN IPv4 targets is displayed.

b. If you chose an L2 VPN RT retrieval record, click on the L2 VPN Route Target tab. A list of L2 VPN targets is displayed.

7

Choose a target and click on the Properties button. The Route Target (Edit) form opens with the General tab displayed.

8

View the following information:

- timestamp of retrieval
- RT
- BGP AS number
- BGP confederation AS number, if applicable
- number of routes
- RT format — AS (2 Byte ASN), AS (4 Byte ASN), or IP Address
- RT AS number, if applicable
- RT extended community value, if applicable
- IP address of the RT, if applicable
- RT community value, if applicable

9

Click on the Advertising Next Hops tab.

10

Choose an entry and click on the Properties button. The Next Hops (Edit) form opens.

11

Perform one of the following:

a. If you chose an IP VPN Route Target, view the following information:
- IP address of the next hop
- IP VPN route count

b. If you chose an L2 VPN Route Target, view the following information:
- IP address of the next hop
- L2 VPN route count

12

Close the Next Hops (Edit) form.

13

Close the Route Target (Edit) form.

14

Close the Route Target Retrieval Record (Edit) form.

15

Close the BGP Network Data form.

END OF STEPS

10.14 To view IP VPN route targets

10.14.1 Steps

1

Perform 10.9 “To retrieve BGP information from a CPAA” (p. 201) to retrieve BGP AS information from a CPAA.

2

Choose Tools→Route Analysis→BGP Network Data from the NFM-P main menu. The BGP Network Data form opens.

3

Choose IPv4 VPN Route Target (CPAM: Topology) from the object drop-down menu.

4

Click on the Search button. A list of timestamped VPN IPv4 RT entries appears.

5

Choose an entry and click on the Properties button. The IP VPN Route Target (Edit) form opens with the General tab displayed.

6

View the following information:

- timestamp of retrieval
- RT
- BGP AS number
- BGP confederation AS number, if applicable
- number of routes
- RT format — AS (2 Byte ASN), AS (4 Byte ASN), or IP Address
- RT AS number, if applicable
- RT extended community value, if applicable
- IP address of the RT, if applicable
- RT community value, if applicable

7

Click on the Advertising Next Hops tab.

8

Choose an entry and click on the Properties button. The Next Hops (Edit) form opens.

9

View the following information:

- IP address of the next hop
- VPN IPv4 route count

10

Close the Next Hops (Edit) form.

11

Close the IP VPN Route Target (Edit) form.

12

Close the BGP Network Data form.

END OF STEPS

10.15 To view L2-VPN route targets

10.15.1 Steps

1

Perform 10.9 “To retrieve BGP information from a CPAA” (p. 201) to retrieve BGP AS information from a CPAA.

2

Choose Tools→Route Analysis→BGP Network Data from the NFM-P main menu. The BGP Network Data form opens.

3

Choose L2-VPN Route Target (CPAM: Topology) from the object drop-down menu.

4

Click on the Search button. A list of timestamped L2-VPN RT entries appears.

5

Choose an entry and click on the Properties button. The L2-VPN Route Target (Edit) form opens with the General tab displayed.

6

View the following information:

- RT
- CPAA AS number
- CPAA confederation number, if applicable
- number of routes
- timestamp of retrieval
- RT format — AS (2 Byte ASN), AS (4 Byte ASN), or IP Address
- RT AS value, if applicable
- RT extended community value, if applicable
- IP address of the RT, if applicable
- RT community value, if applicable

7

Click on the Advertising Next Hops tab.

8

Choose an entry and click on the Properties button. The Next Hops (Edit) form opens.

9

View the following information:

- IP address of the next hop
- L2-VPN route count

10

Close the Next Hops (Edit) form.

11

Close the IP VPN Route Target (Edit) form.

12

Close the BGP Network Data form.

END OF STEPS

10.16 To view BGP AS path topology

10.16.1 Steps

1

Perform 10.9 “To retrieve BGP information from a CPAA” (p. 201) to retrieve BGP AS information from a CPAA.

2

Choose Tools→Route Analysis→BGP Network Data from the NFM-P main menu. The BGP Network Data form opens.

3

Choose BGP Autonomous System (CPAM: Topology) from the object drop-down menu and click on the Search button.

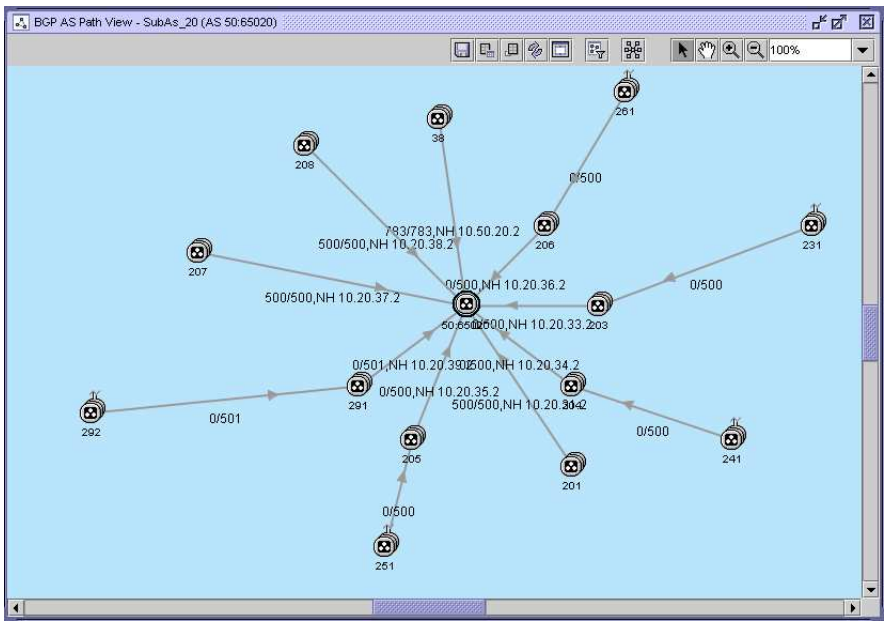
4

Select a non-confederation BGP AS and click on the BGP AS Path View button. A dialog box appears.

5

Click on the Yes button. The BGP AS Path View - *BGP_AS_Name* window opens, as displayed in Figure 10-6, “BGP AS Path View window” (p. 211) .

Figure 10-6 BGP AS Path View window



The text displayed on the topology map under an ASN link is the following:

R / T, NH d.d.d.d

where:

- *R* is the number of BGP routes that originate from the AS
- *T* is the total number of BGP routes
- *NH d.d.d.d* is the IP address of the next hop

For example, 8/200000, NH 25.1.1.1 indicates that eight BGP routes originate from the ASN, and that the total number of BGP routes is 200 000 BGP. The next hop is 25.1.1.1.

Note: Next hop information is displayed only on links that are one hop away from the BGP CPAA.

The text displayed on the topology map under a BGP CPAA AS icon is the following:

CPAA:ASN

where:

- *CPAA* is the ID of the confederation BGP CPAA, for confederation ASs
- *ASN* is the BGP CPAA AS number, for BGP CPAA ASs

The text displayed on the topology map under a BGP CPAA AS-discovered ASN icon is the following:

ASN

where:

- *ASN* is the AS number of the autonomous system discovered by the BGP CPAA

6

Configure the BGP AS path view filter to adjust the maximum number of ASs and number of hops displayed on the map, if necessary. Perform the following:

1. Click on the Configure Display Filter button at the top of the display window. The Configure Display Filter form opens.
2. Configure the parameters:
   - Maximum Number of ASes — the maximum number of ASs to display on the map
   - Maximum Number of Hops From This AS — the maximum number of hops from the CPAA-monitored BGP AS to display on the map
3. Click on the OK button. The Configure Display Filter form closes.
4. Click on the Reload topology view from database button at the top of the display window. A dialog box appears.
5. Click on the Yes button. The dialog box closes and the topology view is reloaded with the filter parameters applied.

7

Double-click on an ASN icon. The ASN (Edit) form opens.

8

View the following ASN information:

- the discovered AS number
- the BGP CPAA that discovered the AS
- the confederation BGP AS number that discovered the AS, if applicable
- segment type:
  - SET — unordered set of ASs that a route in the UPDATE message has traversed
  - SEQUENCE — ordered set of ASs that a route in the UPDATE message has traversed
  - CONF-SEQ — ordered set of member-AS numbers in the confederation that the UPDATE message has traversed
  - CONF-SET — unordered set of member-AS numbers in the confederation that the UPDATE message has traversed
- indicator of whether the value configured for the Depth Value for Retrieve AS Path parameter has been met
- the number BGP routes that originate from the AS
- the number of hops away from the BGP CPAA

9

Close the ASN (Edit) form.

10

Double-click on an ASN link. The ASN Link (Edit) form opens.

11

View the following ASN link information:

- the AS numbers of the originating AS and terminating AS
- the BGP CPAA that discovered the AS
- the confederation BGP AS number that discovered the AS, if applicable
- the next hop, if the AS is one hop away from the BGP CPAA
- the number BGP routes that originate from the AS
- the number of hops away from the BGP CPAA

12

Close the ASN Link (Edit) form.

13

Close the BGP AS Path View - *BGP_AS_Name* window.

14

Close the BGP Network Data form.

END OF STEPS

10.17 To view corrupted BGP update records

10.17.1 When to use

Perform this procedure to view details of a corrupted BGP update when a CorruptedBgpUpdate alarm is raised against a BGP AS.

10.17.2 Steps

1

Choose Tools→Route Analysis→BGP Network Data from the NFM-P main menu. The BGP Network Data form opens.

2

Choose BGP Autonomous System (CPAM: Topology) from the object drop-down menu and click on the Search button.

3

Choose an alarmed entry and click on the Properties button. The BGP Autonomous System (Edit) form opens.

4

Click on the Corrupted BGP Update Records tab.

5

Choose a corrupted BGP update record from the list and click on the Properties button to view details of the corrupted BGP update.

END OF STEPS

10.18 To view CPAA update times information

10.18.1 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.

2

Click on the Select Object Type and click on CPAA (CPAM: Topology) and click on the Search button.

3

Choose an entry and click on the Properties button. The CPAA (Edit) form opens.

4

Click on the Update Times tab.

5

View the following BGP update time information for:

- BGP AS path data
- BGP RIB information
- BGP IP VPN route targets

6

Close the CPAA (Edit) form.

7

Close the Admin Domains / CPAAs form.

END OF STEPS

10.19 To view BGP routes

10.19.1 Steps

1

Choose Tools→Route Analysis→IGP Topology→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate IGP topology map opens.

2

Right-click on a router and choose BGP→Show Routes from the contextual menu. The CPAM BGP Show Routes form opens with the General tab displayed.

3

Perform one of the following:

a. Enter ? in the parameter field and click on the OK button to view a list of valid CLI parameters, if necessary. Close the CPAM BGP Show Routes form and repeat Step 2 and Step 3 b .

b. Enter a CLI parameter and click on the OK button. The BGP routes for the selected router are displayed in CLI output format.

4

Close the CPAM BGP Show Routes form.

5

Close the topology map.

END OF STEPS

10.20 To view BGP paths

10.20.1 Steps

1

Choose Tools→Route Analysis→IGP Topology→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate IGP topology map opens.

2

Right-click on a router and choose BGP→Show Paths from the contextual menu. The CPAM BGP Show Paths form opens with the BGP paths for the selected router are displayed in CLI output format.

3

Close the CPAM BGP Show Paths form.

4

Close the topology map.

END OF STEPS

10.21 To navigate to PE routers advertising an RT on a topology map

10.21.1 Steps

1

Choose Tools→Route Analysis→BGP Network Data from the NFM-P main menu. The BGP Network Data form opens.

2

Choose Route Target Retrieval Record (CPAM: Topology) from the object drop-down menu and click on the Search button. A list of timestamped RT retrieval record entries appears.

3

Choose an entry and click on the Properties button. The Route Target Retrieval Record (Edit) form appears with the General tab displayed.

4

Perform one of the following:

a. If you chose a VPN IPv4 RT retrieval record, click on the IP VPN Route Target tab. A list of VPN IPv4 targets is displayed.

b. If you chose an L2 VPN RT retrieval record, click on the L2 VPN Route Target tab. A list of L2 VPN targets is displayed.

5

Select a target from the list, click on the Navigate button, and choose one of the following options:

- IGP View
- ISIS View
- OSPF View

6

The specified topology map opens with the next hop highlighted.

7

Close the topology map.

8

Close the Route Target Retrieval Record (Edit) form.

9

Close the BGP Network Data form.

END OF STEPS

10.22 To highlight advertising routers for BGP prefixes

10.22.1 Steps

1

Choose Tools→Route Analysis→IGP Topology→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate IGP topology map opens.

2

Right-click on the map and choose Highlight BGP/IPV4/VpnIpV4 Advertising Router. The Highlight BGP/IPV4/VpnIpV4 Advertising Router form opens.

3

Click on the Select button next to the BGP AS parameter, if necessary. The Select BGP AS form opens.

4

Specify a filter for the search, if required, and click on the Search button. A list of BGP AS numbers appears.

5

Choose an entry and click on the OK button. The Select BGP AS form closes and the Highlight BGP/IPV4/VpnIpV4 Advertising Router form refreshes with the BGP AS number.

6

Configure the parameters:

- IP Address
- Prefix Length
- Prefix Type

7

Click on the OK button. The Highlight BGP/IPV4/VpnIpV4 Advertising Router form closes and the routers that advertise the specified prefix are highlighted on the topology map.

8

Click on the Legend button at the top of the topology map and choose Highlight Sessions from the contextual menu. The Legend - IGP Topology form opens with the Highlight Sessions tab

displayed. See 7.32 “To manage active highlights on a topology map” (p. 123) for information about how to manage active highlights on a topology map.

9

Close the topology map.

END OF STEPS

11 BGP statistics

11.1 BGP statistics overview

11.1.1 Introduction to CPAM BGP statistics

The CPAM retrieves BGP MIB statistics collected by the CPAA. You can use the CPAM to view statistics data in tabular or graphical form, save the tabular or graphical data to a file in various formats, and export the statistics data to OSS applications.

You can view BGP statistics from the Statistics tab of a monitored object properties form.

The NFM-P plotter is used to plot all of the statistics in both historical and real-time mode. The CPAM supports all of the capabilities of the NFM-P plotter for BGP statistics.

All of the restrictions of the NFM-P plotter apply to BGP statistics, including the total number of CPAM statistics that can be collected by the NFM-P, and the minimum number of days the statistics are maintained.

Note: The CPAM statistics collection constraints must be considered when you configure statistics collection policies. See the 11.1.2 “Statistics scalability” (p. 219) section for more information.

Before the CPAA can collect statistics, you must configure statistics MIB policies that specify the following:

- the objects from which to collect statistics
- the counters to collect
- the rate of collection
- the length of time that the CPAM saves the statistics

See 11.2 “CPAM MIB statistics policies” (p. 220) for more information about statistics MIB policies.

11.1.2 Statistics scalability

The CPAM supports the large-scale collection of statistics from the managed network. Performance, accounting, and server performance statistics can be collected according to a schedule and are stored for a configurable period. The following formula is used to calculate the storage capacity that scheduled collection consumes:

```
(number of objects to collect from) x (collection frequency) x (retention period)
```

When a statistics collection policy or an accounting policy applies to many objects, the collection interval must be large enough to collect the data. If the statistics collection time exceeds the collection interval, the CPAM raises an alarm.

Note: To prevent statistics loss and performance degradation, Nokia recommends that you stay within the specified maximum guidelines and ensure that each collection interval is long enough for the number of statistics to be collected during the interval.

11.1.3 Graphical statistics view

Statistics can be viewed in a graph using the NFM-P statistics plotter. The plotter can display multiple performance, accounting, and server performance statistics simultaneously using dual axes. The plotter also provides a numerical value for each point on the graph.

Each NFM-P client can open up to five statistics plotters, and each plotter can simultaneously plot up to four counters. Plotters can have independent Y axes on the left and right sides of a graph, and any counter can be assigned to one of the Y axes.

A plotter can plot historical or real-time statistics. Historical plots use stored statistics from earlier collections. The plotter automatically plots all of the stored values for the specified counter. Real-time plots collect statistics while the plotter window is open and plot the data as the data is collected.

For real-time statistics, when multiple NFM-P clients each have multiple open plotters that are displaying multiple counters, a high volume of statistics is collected from the CPAAs.

Note: If the collection for many of the plotters is from the same CPAA, the CPAA is polled independently for each plotter, which may degrade performance. You can use a scope of command role to limit plotter access to specific NFM-P user groups.

11.2 CPAM MIB statistics policies

11.2.1 Overview of CPAM MIB statistics policies

The collection of BGP statistics is controlled by MIB statistics polices that specify an administrative state, polling synchronization start time, and collection interval. The two types of MIB statistics policies are:

- NE MIB statistics policies—apply to all of the NE objects (RTs and next hops, or originating AS) of the specified types
- specific MIB statistics policies—apply to a specific NE object

Note: Nokia recommends that you configure specific MIB statistics policies for BGP collection to reduce the large number of statistics that can be collected for a global policy or an NE MIB statistics policy.

Each type of MIB statistics policy contains a list of MIB entry policies. A MIB entry policy defines the collection criteria for a specific MIB row. In an NE MIB policy, a MIB entry policy applies to all of the objects on the NE that use the MIB entry. In a specific MIB policy, the MIB entry policy applies only to the specified objects on the NE.

If the statistics collection time required for a MIB entry exceeds the collection interval specified in the MIB statistics policy, the CPAM raises an alarm. You can change the polling interval for a statistics class to prevent this occurrence.

11.2.2 Specific MIB statistics policies

A specific MIB statistics policy defines the collection of selected performance statistics from specific objects on specific NEs for more statistics collection granularity. For example, to collect BGP statistics for BGP routes churn in one originated AS and BGP routes churn in another originated AS, you can specify two policies that specify different collection intervals, and the originated AS to which each policy applies.

The settings in a specific MIB statistics policy override the settings in an NE MIB statistics policy, and can be used to disable statistics collection for specific objects. For example, you enable statistics collection globally for a CPAA using an NE MIB statistics policy, and then disable the collection of specific statistics using a specific MIB statistics policy.

Note: Nokia recommends that you use specific MIB statistics policies for BGP statistics.

11.2.3 NE MIB statistics policies

An NE MIB statistics policy defines the global collection of specific statistics on specific CPAAs. In this scenario, configure NE MIB policies rather than specific MIB policies for more efficiency and fewer collection resources.

After an NE MIB statistics policy is applied to a CPAA, statistics are collected for all of the objects on the CPAA, except for objects that have a specific MIB statistics policy. As a result, statistics cannot be collected twice, that is, once by the NE MIB policy and once by the specific MIB policy.

Each CPAA requires an NE MIB statistics policy. The CPAM has a default policy that is applied to a CPAA automatically when an NE MIB statistics policy is not specified. The collection interval for each counter in the default policy is 15 minutes. Collection is disabled by default to conserve NE resources.

11.3 CPAM BGP statistics

11.3.1 Types of CPAM BGP statistics

The different types of BGP statistics that are collected by the CPAA are:

- statistics for global BGP
- statistics for BGP Route Target
- statistics per Next Hop in global BGP
- statistics per Next Hop for each Route Target
- statistics for BGP Originated AS

11.3.2 Global BGP

The CPAA collects the following statistics for global BGP and for each RT:

- total number of sub-AS internal BGP routes
- total number of confederation internal BGP routes (only for global BGP)
- total number of external BGP routes
- number of BGP routes churn (added or withdrawn)

- number of BGP routes added
- number of BGP routes withdrawn
- number of flapped BGP routes (flap is defined as a route added after being withdrawn)
- number of changed Next-Hop
- number of changed LOCAL-PREF
- number of changed MED
- number of changed COMMUNITY
- number of changed AS-PATH

11.3.3 Next hop for global BGP and per RT

The CPAA collects the following statistics per Next Hop for global BGP and per RT:

- total number BGP routes
- number of BGP routes added or withdrawn
- number of BGP routes added
- number of BGP routes withdrawn
- number of flapped BGP routes (flap is defined as routes added or withdrawn)
- number of changed LOCAL-PREF
- number of changed MED
- number of changed COMMUNITY
- number of changed AS-PATH

Note: BGP statistics are identified by (RT:NH), where the where RT is the Route Target and NH is the Next Hop. For global BGP, the RT is 0. When the NH is 0, the statistics are aggregated for all of the next hops. The statistics for each next hop are identified by a none-zero NH. A non-zero RT specifies the specific RT.

Flaps are detected within a 2-minute interval. The counter starts when a route is withdrawn.

11.3.4 BGP originated AS

The CPAA collects the following statistics for each originated AS:

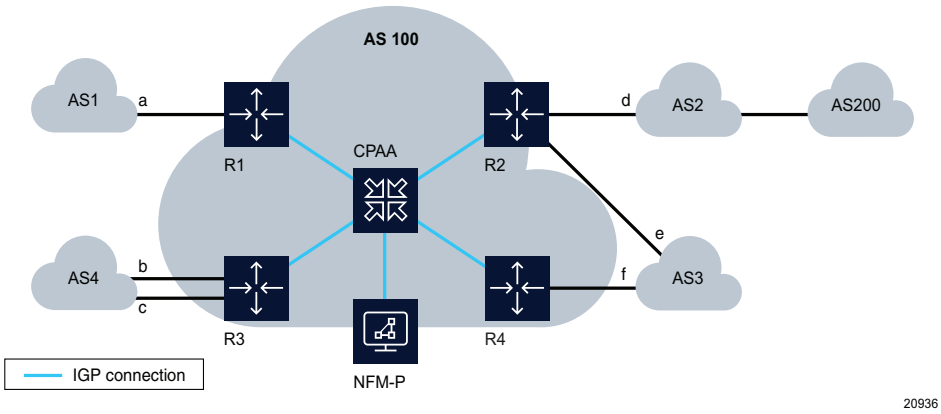
- total number of originated BGP routes
- number of BGP routes churn (added or withdrawn)
- number of BGP routes added
- number of BGP routes withdrawn

11.4 Sample BGP network statistics configuration

11.4.1 Overview

The following figure shows a sample BGP network:

Figure 11-1 Sample BGP network



In Figure 11-1, “Sample BGP network” (p. 223) , *a*, *b*, *c*, *d*, *e*, and *f* identify interface IP addresses (Next Hop). AS100 receives VPN-IPv4 routes from AS1, AS2, AS3, AS4, and AS200 for two route targets, RT1 and RT2. It also receives IPv4 from AS1, AS2, AS3, AS4, and AS200. In this example, ASBR routers R1, R2, R3, and R4 do not use the BGP routing command next-hop-self—they do not send their own IP address as the next hop.

11.4.2 BGP statistics for RT and next hops

The CPAA collects the BGP statistics listed in 11.3.2 “Global BGP” (p. 221) and 11.3.3 “Next hop for global BGP and per RT” (p. 222) for each Next Hop for global BGP and for each RT.

BGP statistics are collected for the following:

- target 0:0
  - NH=0.0.0.0 (aggregated statistics for NH=*a*, *b*,*c*, and *d*)
  - NH=*a*
  - NH=*b*
  - NH=*c*
  - NH=*d*
  - NH=*e*
  - NH=*f*
- target RT
  - NH=0.0.0.0 (aggregated statistics for NH=*a*, *b*,*c*, and *d*)
  - NH=*a*
  - NH=*b*
  - NH=*c*
  - NH=*d*
  - NH=*e*
  - NH=*f*
- target RT

  - NH=0.0.0.0 (aggregated statistics for NH=*a*, *b*,*c*, and *d*)
  - NH=*a*
  - NH=*b*
  - NH=*c*
  - NH=*d*
  - NH=*e*
  - NH=*f*
- target RT
  - NH=0.0.0.0 (aggregated statistics for NH=*a*, *b*,*c*, and *d*)
  - NH=a
  - NH=b
  - NH=c
  - NH=d
  - NH=e
  - NH=f
- target RT
  - NH=0.0.0.0 (aggregated statistics for NH=*a*, *b*,*c*, and *d*)
  - NH=a
  - NH=b
  - NH=c
  - NH=d
  - NH=e
  - NH=f

11.4.3 BGP statistics for originated AS

The CPAA collects the statistics, which are listed in 11.3.4 “BGP originated AS” (p. 222) for each originated AS. If autonomous system AS200 advertises BGP routes 10.1.1.1/32 and 10.2.2.2/32 to AS100, the CPAA receives these two routes and collect the BGP statistics for AS200 as the originating AS.

11.5 Workflow for BGP statistics

11.5.1 Stages

1

Configure a MIB policy for statistics collection. See 11.6 “To manage a specific MIB policy for BGP statistics collection” (p. 225) for more information.

2

Configure a policy for statistics retention. See 11.7 “To create a retention policy for BGP statistics” (p. 227) for more information.

3

Browse collected BGP statistics for:

- BGP Stats-Route Target and Next Hops
- BGP Stats-Originating AS

4

Plot the statistics graphically:

1. Configure the global parameters for statistics graphing. See 11.8 “To configure the global parameters for statistics graphing” (p. 228) for more information.
2. Configure and plot a statistics graph. See 11.9 “To configure and plot a statistics graph” (p. 228) for more information.

11.6 To manage a specific MIB policy for BGP statistics collection

11.6.1 When to use

Perform this procedure to configure a policy for BGP statistics collection for a specific CPAA MIB object.

Note: You can also create a generic MIB policy.

11.6.2 Steps

1

Choose Tools→Statistics→MIB Policies from the NFM-P main menu. The Manage MIB Statistics Policies form opens.

2

Choose Specific MIB Statistics Policy (SNMP) from the object menu.

3

Perform one of the following:

a. Modify a MIB statistics policy.

1. Specify a filter to create a filtered list of MIB statistics policies. A list of MIB statistics policies is displayed.
2. Choose a MIB statistics policy and click on the Properties button. The Specific MIB Statistics Policy form (Edit) opens.

Note: When you change a MIB statistics policy for the statistics class of an object, the same changes apply to all of the other objects that use the same statistics class.

b. Click on the Create button to create a MIB statistics policy. The Specific MIB Statistics Policy (Create) form opens.

4

Configure the parameters:

- Auto-Assign ID
- Policy ID
- Name
- Polling Synchronization Time
- Polling Admin State

5

Click on the Select button for the Monitored Class Name. The Specific Stats Poller Policy form opens.

6

Choose one of the following object types and click on the OK button:

- BGP Stats-Originated AS (CPAM:Topology)
- BGP Stats-Route Target and Next Hops (CPAM:Topology)

The Specific Stats Poller Policy form closes and the Specific MIB Statistics Policy form reappears with the object type displayed in the Monitored Class Name field.

7

Click on the Apply button. The Specific MIB Statistics Policy form refreshes to display additional tab buttons.

8

Click on the Monitored Objects tab button.

9

Click on the Add button. The Select *monitored_object* for Specific MIB Statistics Policy form opens.

10

Configure the filter criteria and click on the Search button. A list of monitored objects is displayed.

11

Choose one or more objects and click on the OK button. The Select *monitored_object* for Specific MIB Statistics Policy form closes and the Specific MIB Statistics Policy form reappears with the selected objects listed.

12

Click on the OK button. The Specific MIB Statistics Policy form closes and the Manage MIB Statistics Policies form reappears.

13

Close the Manage MIB Statistics Policies form.

END OF STEPS

11.7 To create a retention policy for BGP statistics

11.7.1 General information

Perform this procedure to configure a policy for statistics retention. By default, statistics are retained for 24 h. You can create a retention policy for each MIB object.

11.7.2 Steps

1

Choose Tools→Statistics→Statistics Browser from the NFM-P main menu. The Browse Statistics form opens.

2

Choose one of the following from the Select Object Type menu:

- BGP Stats-Originated AS (CPAM:Topology)
- BGP Stats-Route Target and Next Hops (CPAM:Topology)

3

Choose Statistics Policy from the Statistics Type menu and click on the Search button.

4

Choose an entry and click on the Properties button. The Statistics Policy - Topology.Bgp*object_type* form opens with the General tab displayed.

5

Configure the parameters:

- Retention Time (hours)
- Administrative State
- Threshold Reporting State

6

Click on the Thresholds tab button. The Thresholds tab contains a threshold parameter for each counter in the statistics class.

7

Configure the threshold parameters. When a statistics counter threshold is exceeded, the CPAM raises a threshold crossing alarm.

8

Click on the OK button. A dialog box opens.

9

Click on the Yes button. The Statistics Policy form closes.

10

Close the Browse Statistics form.

END OF STEPS

11.8 To configure the global parameters for statistics graphing

11.8.1 Steps

1

Choose Tools→Statistics→Statistics Plotter from the NFM-P main menu. The Statistics Plotter form opens.

2

Configure the parameters:

- Default Polling Interval (seconds)
- Maximum Data Retention Time (seconds)

3

Click on the OK button to close the Statistics Plotter form and apply the changes.

END OF STEPS

11.9 To configure and plot a statistics graph

11.9.1 Steps

1

Choose Tools→Statistics→MIB Policies from the NFM-P main menu. The Manage MIB Statistics Policies form opens.

2

Choose Specific MIB Statistics Policy (SNMP) from the object drop-down menu and click on the Search button. A list of policies appears.

3

Choose the policy for which you need to plot a statistics graph and click on the Properties

button. The Specific MIB Statistics Policy (Edit) form opens with the General tab displayed.

Note: You must choose a policy for one of the following monitored class names:

- topology.BgpOriginatedAs
- topology.BgpRoutesNexthHop

4

Click on the Monitored Objects tab button.

5

Choose the object for which you need to plot the statistics and click on the Properties button. The BGP Stats-*Object* (Edit) form opens with the General tab displayed.

6

Click on the Statistics tab button.

7

Click on the Search button to view statistics record entries for scheduled collections of the selected statistics class, or click on the Collect button to perform an on-demand collection and view the current statistics for the selected statistics class.

8

Choose a statistics record.

9

Click on the Plotter button and choose New Plot from the contextual menu. The Statistics Plotter form opens.

10

Click on a plot in the Statistics Counter column of the configuration panel and choose a statistics counter from the menu.

11

Add a plot to the statistics plotter. You can duplicate the existing object or choose a new object. If the same object is used, the statistics counter must be unique. If a different object is used, the same statistics counter can be used for each object.

Note: A statistics graph can plot up to four statistics counters. The statistics counters can all be the same when there are four different objects. If only one object is used, each statistics counter must be unique.

a. To add a plot using an object in the list:

1. Choose an entry and click on the Duplicate button. The plot is duplicated in the list.

2. Click on the new plot in the Statistics Counter column and choose a statistics counter from the menu. The counter must be unique.
3. Click on the Y Axis column and choose an axis from the menu.

b. To add a statistics counter using a new object, repeat to Step 1 to Step 9 .

12

To add another plot to the plotter, repeat Step 11 . You can create up to four plots.

Note: Each plot must be unique. The CPAM deletes the older plot if you attempt to create a duplicate a plot in this step.

13

Perform one of the following:

a. To create a real-time statistics graph:
   1. Choose a polling interval from the Real-time Polling Interval drop-down menu, or enter a value between 10 and 60.
   2. Click on the Real-time Plot button. The detail panel displays the plotted statistics using the configured polling interval.

      Note:

      You do not have to stop real-time statistics collection to add or remove plots.
   3. Click on the stop button to pause the real-time statistics collection.

b. To create a graph using historical statistics, click on the Historical Plot button. The statistics are plotted in the detail panel.

14

Perform one or more of the following to view information in the detail panel.

a. To display a tool tip for a plot, move the mouse pointer over the data points in the detail panel. A tool tip identifies the plot number, the statistics collection interval, and the statistics value at that interval.

b. To change the view displayed in the detail panel, click on the green box in the overview panel and drag the box horizontally.

   When the green box is not selected and real-time statistics are being collected, the green box automatically scrolls to display the latest statistics.

c. To turn off autoscrolling, double-click on the green box. The green box changes to red. When the box is red, autoscrolling is turned off and the detail panel remains in the location displayed in the overview panel red box.

d. To resize the objects in the detail panel, click on the Zoom in Tool and Zoom out Tool buttons. Click on the Reset Zoom tool button to return to the default graph view.

e. To display the data points for each plot in the detail panel, select the Markers check box.

f. To display a legend in the detail panel, select the Legend check box.

g. To display the X-axis grid lines, select the Grid X check box. This check box is selected by default.

h. To display the Y1 grid lines, select the Grid Y1 check box. The Y1 axis is displayed on the left side of the detail panel. The grid lines are displayed only if the Y1 axis is in use.

i. To display the Y2 grid lines, select the Grid Y2 check box. The Y2 axis is displayed on the right side of the detail panel. The grid lines are displayed only if the Y2 axis is in use.

j. Perform the following steps to hide or show a plot in the detail panel. This is required when plots in the detail panel overlap.

   1. Choose the plot to hide in the detail panel.
   2. Click in the column heading configuration panel and choose Plot *n* in the menu, where *n* is the plot to hide. The check mark is removed from the plot list, and the plot is removed from the detail and data panels.

      Note:

      Statistics collection does not stop when a plot is hidden.

   3. To show the plot in the detail panel, right-click in the column heading of the data panel and choose Plot *n* from the contextual menu, where *n* is the plot to show. A check mark is displayed beside the plot in the contextual menu and the plot is displayed in the detail and data panels.

15

To clear a plot from the detail panel but keep the plot in the configuration panel so that the plot can be used to create a new plot:

1. Choose the object in the list and click on the Clear button. The plot is deleted from the detail and data panels.
2. Click on the plot in the Statistics Counter column and choose a unique statistics counter from the menu.
3. Click on the Y Axis column and choose an axis from the menu.

16

To remove a plot from the detail and data panels, select the object in the list and click on the Remove button. The plot is deleted from the detail and data panels.

17

Perform one of the following steps, if required.

a. To switch from a real-time statistics graph to a historical statistics graph, click on the Stop button and click on the Historical Plot button. The detail panel clears and the statistics are plotted in the detail panel.

b. To switch from a historical statistics graph to a real-time statistics graph, choose a polling interval from the real-time polling interval drop-down menu or enter a value between 10 and 3600 seconds and click on the Real-time Plot button. The detail panel clears and real-time statistics plotting begins.

18

Save the statistics graph results, if required.

Note: Only the detail that appears in the detail panel is saved. To change the view in the detail panel before you save the results, use the overview panel or the zoom buttons. If the Legend check box is selected, the legend is saved with the statistics graph results.

1. Click on the Save Current View button. The Save as form appears.
2. Specify a directory in which to save the statistics graph using the Save In parameter. The Save In form opens.
3. Enter a filename in the File Name field.
4. Choose JPG or PNG from the Type of File drop-down menu.
5. Click on the Save button. The Save as form closes and the graph is saved in the specified JPG or PNG file.

19

Save the statistics table results, if required. All of the statistics in the data panel are saved.

1. Right-click on the plot value list heading and choose Save To File from the contextual menu. The Save form opens.
2. Specify a directory in which to save the statistics table using the Save In parameter. The Save In form opens.
3. Enter a filename using the File Name field.
4. Choose HTML or CSV from the Type of File drop-down menu.
5. Click on the Save button. The Save form closes and the contents of the plot value list are saved in the specified file.

20

Close the Statistics Plotter form.

Note: The Statistics Plotter form cannot be saved. When you close a Statistics Plotter form, the data in the form is deleted.

END OF STEPS

11.10 To plot BGP event statistics

11.10.1 Steps

1

Perform one of the following:

a. Choose Tools→Route Analysis→Impact Analysis from the NFM-P main menu. The Impact Analysis form opens. Go to Step 2 .

b. Choose Tools→Statistics→Server Performance Statistics from the NFM-P main menu. The

Server Performance Statistics form opens. Go to Step 4 .

2

Choose BGP Impact Analysis (CPAM: Topology) from the object drop-down menu.

3

Click on the BGP Event Stats Plotter button. The Statistics Plotter form opens with the impact analysis statistics plotted. Go to Step 8 .

Note: For information about configuring a BGP Impact Analysis, see 18.7 “To configure a historical BGP impact analysis” (p. 358) .

4

Choose CPAM BGP AS Events (NFM-P Performance Statistics) from the object drop-down menu.

5

Click on the Search button. A list of CPAM BGP AS Events appears.

6

Click on the More Actions button and choose Plotter→New Plot. The Statistics Plotter form opens with the CPAM BGP AS Events statistics plotted.

7

Click on the Historical Plot button. The CPAM BGP AS Events statistics plotted.

8

As required, use the statistics plotter as described in 11.9 “To configure and plot a statistics graph” (p. 228) .

9

As required, click on the Launch button and choose Top 100 Change Contributers→Next Hop. The Top 100 Contributing Next Hops For All Events form opens.

10

Review the information and close the form.

11

As required, click on the Launch button and choose Top 100 Change Contributers→Prefix.The Top 100 Contributing Prefixes For All Events form opens.

12

Review the information and close the form.

13

As required, click on the Launch button and choose Top 100 Change Contributers→Neighbor AS. The Top 100 Contributing Neighbor Autonomous Systems For All Events form opens.

14

Review the information and close the form.

15

If using a VPN statistics counter, click on the Launch button and choose Top 100 Change Contributers→Route Target. The Top 100 Contributing Route Targets For VPN All Events form opens.

16

Perform one of the following:

a. Review the information and close the form.

b. Select a Route Target from the list and click on the BGP Impact Analysis button. The BGP Impact Analysis form opens. See 18.7 “To configure a historical BGP impact analysis” (p. 358) for information about performing a BGP Impact Analysis.

17

As required, click on the Launch button and choose BGP Impact Analysis. The Impact Analysis form opens. See 18.7 “To configure a historical BGP impact analysis” (p. 358) for information about Performing BGP Impact Analysis.

18

Close the Statistics Plotter form.

19

Close Impact Analysis form.

END OF STEPS

12 BGP route profiles

12.1 BGP route profiles overview

12.1.1 CPAM support for BGP route profiles

The CPAM supports the creation of BGP route profiles, which are used to monitor BGP prefix updates according to user-defined rules. The CPAM can support up to 5000 BGP route profiles.

12.2 Workflow for BGP route profiles configuration

12.2.1 Stages

1

Create a BGP route profile. See 12.3 “To create a BGP route profile” (p. 236) for more information.

2

As required, configure the BGP route profile to receive JMS-CPAM topic notifications. See 12.4 “To configure a BGP route profile to receive JMS-CPAM topic notifications” (p. 238) for more information.

3

As required, configure the BGP route profile to raise alarms when monitored prefixes become unreachable. See 12.5 “To configure a BGP route profile to raise an unreachable prefix alarm” (p. 238) for more information.

4

As required, retrieve BGP prefixes from the BGP route profile. See 12.6 “To retrieve a filtered BGP prefix list from a BGP route profile” (p. 239) for more information.

5

As required, retrieve BGP events from the BGP route profile. See 12.7 “To configure BGP event retrieval from a BGP route profile” (p. 240) for more information.

6

As required, associate BGP route profiles with a VPRN service, or vice versa. See 12.8 “To associate a VPRN service with a BGP route profile” (p. 241) or 12.9 “To associate a BGP route profile with a VPRN service” (p. 242) for more information.

12.3 To create a BGP route profile

12.3.1 Steps

1

Choose Tools→Route Analysis→Route Profiles from the NFM-P main menu. The Route Profiles form appears.

2

Perform one of the following:

a. Click on the Create button and choose IP VPN BGP Route Profile.

b. Click on the Create button and choose Global BGP Route Profile.

The BGP Route Profile (Create) form opens.

3

Configure the required parameters.

4

Perform one of the following:

a. Select the BGP AS by configuring the Confederation AS Number and AS Number parameters.

b. Select a BGP AS in the BGP AS panel.

Note: Each BGP route profile must be unique. A BGP route profile cannot be created if its parameters are configured to the same values as the parameters of an existing BGP route profile.

5

Perform one of the following:

a. If you chose IP VPN BGP Route Profile in Step 2 , continue to Step 6 .

b. If you chose Global BGP Route Profile in Step 2 , go to Step 14 .

6

Configure the Profile Type parameter.

7

Perform one of the following:

a. If the Profile Type parameter was set to Route Distinguisher Based in Step 6 , continue to Step 8 .

b. If the Profile Type parameter was set to Route Target Based in Step 6 , go to Step 11 .

8

Click on the Route Distinguishers tab and click Add.

9

Configure the Value parameter and click OK.

Note: A maximum of five BGP route profiles can share the same route distinguisher, but their route targets or communities must be unique.

10

To add Route Targets, continue to Step 11 . Otherwise, go to Step 14 .

11

Click on the Route Targets tab and click Add.

12

Configure the Value parameter and click Apply.

Note: A maximum of five BGP route profiles can share the same route target, but their communities must be unique.

13

As required, repeat Step 12 to add additional Route Targets, up to a maximum of 20. Click OK when finished.

14

Click on the Communities tab and click Add.

15

Configure the Value parameter and click Apply.

16

If creating an IP VPN BGP route profile, you may repeat Step 15 to add additional Communities, up to a maximum of 20. Click OK when finished.

17

Save your changes and close the form.

END OF STEPS

12.4 To configure a BGP route profile to receive JMS-CPAM topic notifications

12.4.1 General information

When administratively up, the BGP route profiles tag incoming BGP events that match defined profiles. Other applications can then register with the NFM-P JMS server to receive a notification each time a BGP event matches a defined BGP route profile. These notifications contain the name of the profile which has tagged events and a timestamp for the last event that was tagged. A subscription to the 5650-CPAM-topic-xml JMS topic is required in order to receive the notifications. The amount of notifications received can be throttled on a per-profile basis.

12.4.2 Steps

1

Choose Tools→Route Analysis→Route Profiles from the NFM-P main menu. The Route Profiles form opens.

2

Choose Global BGP Route Profiles or IP VPN BGP Route Profiles and click Search.

3

Choose an entry and click Properties. The BGP Route Profile (Edit) form opens.

4

Click on the Actions tab and enable the JMS - CPAM Topic Notifications parameter.

5

Configure the JMS Notification Throttle (sec) parameters

6

Save your changes and close the forms.

END OF STEPS

12.5 To configure a BGP route profile to raise an unreachable prefix alarm

12.5.1 Steps

1

Choose Tools→Route Analysis→Route Profiles from the NFM-P main menu. The Route Profiles form opens.

2

Choose Global BGP Route Profiles or IP VPN BGP Route Profiles and click Search.

3

Choose an entry and click Properties. The BGP Route Profile (Edit) form opens.

4

Click on the Actions tab and enable the Unreachable parameter.

5

Save your changes and close the forms.

End of steps

12.6 To retrieve a filtered BGP prefix list from a BGP route profile

12.6.1 General information

All matching BGP prefixes can be retrieved from the BGP route profile. Each retrieval lists the BGP prefixes and AS paths that match the BGP route profile from which the retrieval was triggered. A list of all retrievals triggered from each BGP route profile is also maintained. For more information about BGP prefixes, see Chapter 9, “Prefix lists” .

12.6.2 Steps

1

Choose Tools→Route Analysis→Route Profiles from the NFM-P main menu. The Route Profiles form opens.

2

Choose Global BGP Route Profiles or IP VPN BGP Route Profiles and click Search.

3

Choose an entry and click Properties. The BGP Route Profile (Edit) form opens.

4

Click on the BGP Prefix Retrieval tab.

5

Click Retrieve BGP Prefix.

6

Choose an entry and click Properties. The Retrieved BGP Prefixes (Edit) form opens.

7

Click on the Prefixes tab and click Search.

8

Choose an entry and click Properties. The BGP Prefix (Edit) form opens.

9

Review the prefix details and close the form.

10

Click on the BGP AS-PATH tab and click Search.

11

Choose an entry and click Properties. The BGP AS-Path (Edit) form opens.

12

Review the path details and close the form.

13

Save your changes and close the forms.

END OF STEPS

12.7 To configure BGP event retrieval from a BGP route profile

12.7.1 General information

BGP route profiles can be used to retrieve matching BGP events. For more information about BGP event retrieval, see Chapter 18, “Impact analysis” .

12.7.2 Steps

1

Choose Tools→Route Analysis→Route Profiles from the NFM-P main menu. The Route Profiles form opens.

2

Choose Global BGP Route Profiles or IP VPN BGP Route Profiles and click Search.

3

Choose an entry and click Properties. The BGP Route Profile (Edit) form opens.

4

Click View BGP Routing Events. The BGP Profiled Event Retrieval Filter form opens.

5

Configure the Retrieve Last Event and Time Interval Type parameters.

6

Perform one of the following:

a. If you selected Rewind From/To Interval, configure the Start Time and End Time parameters.

b. If you selected Rewind From Current Time, configure the Time Interval (in minutes) parameter.

7

Click View BGP Events. The BGP Events form opens.

8

Click Search.

9

Choose an entry and click Properties. The BGP Prefix Event form opens.

10

Review the event details and close the form.

11

Save your changes and close the forms.

END OF STEPS

12.8 To associate a VPRN service with a BGP route profile

12.8.1 General information

Events retrieved by a BGP route profile may match events from one or more VPRN services. A profile-service association will associate committed profiles with VPRN services that feature matching rules. These associations can be freely deleted after creation.

12.8.2 Steps

1

Choose Tools→Route Analysis→Route Profiles from the NFM-P main menu. The Route Profiles form opens.

2

Choose IP VPN BGP Route Profiles and click Search.

3

Choose an entry and click Properties. The BGP Route Profile (Edit) form opens.

4

Click on the Associated Services tab and click Create. The VPN BGP Route Profile Service Association (Create) form opens.

5

Configure the Validate Service Against Profile parameter.

6

Perform one of the following:

a. Select the VPRN service by configuring the parameters:
   - SVC Mgr Service ID
   - Service ID
   - Service Name

b. Select a VPRN service in the service panel.

7

Save your changes and close the forms.

END OF STEPS

12.9 To associate a BGP route profile with a VPRN service

12.9.1 General information

Events retrieved by one or more VPRN services may match events from a BGP route profile. A profile-service association will associate VPRN services with committed profiles that feature matching rules. These associations can be freely deleted after creation.

12.9.2 Steps

1

Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.

2

Choose VPRN Service (VPRN) and click Search.

3

Choose an entry and click Properties. The VPRN Service (Edit) form opens.

4

Click CPAM and choose BGP Route Profiles. The BGP Route Profiles - VPRN form opens.

5

Perform one of the following:

a. Click Create and choose IP VPN RD-Based Profile. The Create Route Profile from Service - VPRN form opens. Continue to Step 6 .

b. Click Create and choose IP VPN RT-Based Profile. The Create Route Profile from Service - VPRN form opens. Go to Step 8 .

6

Choose a BGP AS and a route distinguisher.

7

Choose one or more route targets and click the right arrow. Go to Step 10 .

8

Choose a BGP AS and a route target.

9

Click Create. The IP VPN BGP Route Profile (Create) form opens.

10

Click on the Communities tab and click Add.

11

Configure the Value parameter and click Apply.

12

Repeat Step 11 to add additional Communities, up to a maximum of 15. Click OK when finished.

13

Save your changes and close the forms.

END OF STEPS

Part V: Fault management

Overview

Purpose

This volume provides fault management information.

Contents

13 OAM diagnostics

13.1 OAM diagnostics overview

13.1.1 Introduction

You can use the CPAM to create IP, LSP, and P2MP LSP path monitor test policies and to highlight OAM diagnostics results on topology maps. See Chapter 4, “Topology management” for information about topology maps and highlighting objects on maps. See “Service Test Manager” in the *NSP NFM-P Classic Management User Guide* for information about STM policies and test suites.

13.2 IP, LSP, and P2MP LSP path test policies

13.2.1 Auto OAM for path monitors

You can create test policies to associate to an IP, LSP, or P2MP LSP path monitor. The tests that you define in the policy are executed when the path reroutes. An OAM execution policy controls the automatic execution of tests.

For IP path monitor test policies, you can define ICMP ping and ICMP trace tests. For LSP path monitor test policies, you can define LSP ping and LSP trace tests. For P2MP LSP path monitors, you can define P2MP LSP ping and P2MP LSP trace tests.

IP, LSP, and P2MP LSP path monitor tests run only on operational IP, LSP, and P2MP LSP paths. Additionally, LSP path monitor tests run only on active LSP paths.

IP, LSP, and P2MP LSP path monitor tests within a test suite are executed in the following ways:

- Automatically, using the Auto OAM function. The specified tests are performed when an active path reroutes.
- When you capture a path on the IP, LSP, or P2MP LSP path monitor configuration form.
- When you execute the associated test suite.
- When you manually run the test from the IP, LSP, or P2MP LSP path monitor configuration form.

The CPAM automatically creates a test suite when you assign an STM test policy to an IP, LSP, or P2MP LSP path monitor.

13.2.2 Execution policies

Execution policies allow you to define the parameters that control the execution of the OAM tests. You can associate an execution policy to an IP, LSP, or P2MP LSP path monitor. Execution policies are specific to the CPAM feature set, and are only applied to Auto OAM tests for path monitors. See 13.9 “To configure an OAM test execution policy” (p. 261) for more information.

13.2.3 Auto OAM state

The results of Auto OAM tests are displayed on the Path Monitor form, under the Auto OAM tab. In addition, the Auto OAM state for each path record is displayed on the Path History tab of the Path Monitor form. The following Auto OAM states may be displayed:

- Not Applicable

  Tests may not be fully configured for the path monitor; for instance, an STM test policy is not selected. Alternatively, the path record is not for an active path, or the associated LSP is administratively down.

- Dropped

  The internal queue associated with test execution is full, and retries are not successful. After a preset number of retries, the test is dropped. The Priority parameter value configured in the execution policy affects this process. See 13.9 “To configure an OAM test execution policy” (p. 261). Alternatively, there may be duplicate path records. OAM tests for a duplicate path record are dropped.

13.3 OAM trace highlights

13.3.1 General information

OAM trace results include several network components. In the case of multicast trace, the paths from the source to the leaves are listed in different windows—one window for each trace from the source to a leaf router.

13.3.2 Traceroute

The shortest path calculation is based the results of an ICMP trace returned from a 7450 ESS or 7750 SR ICMP trace operation. The calculation does not assess the routing policies and static route configured for the routers in the path. The traceries diagnostic helps to ensure that the same path is used for the planned and the actual paths.

13.3.3 LSP trace

You can highlight the results of an LSP trace diagnostic on the IGP topology map. An LSP trace applies to both LDP and RSVP LSP.

13.3.4 Multicast trace

You can highlight the results of a multicast trace (Mtrace) diagnostic on any topology map. The highlights help to identify the multicast tree for a source and group.

13.4 Global Info tables on highlighted OAM results

13.4.1 General information

You can use the Global Info Tables option on the topology map to configure an info table that displays information about highlighted OAM test results on the map. You can view attributes for the following highlights on the topology maps:

- ICMP ping results
- ICMP trace results
- LSP ping results
- LSP trace results
- P2MP LSP ping results
- P2MP LSP trace results
- tested entity results

See 7.35 “To use the Global Info Tables button” (p. 125) for information about how to configure Global Info Tables. See 7.37 “To apply an info table configuration to a map highlight” (p. 126) for information about how to apply an info table to an OAM highlight on the topology map.

13.5 Workflow for OAM diagnostics

13.5.1 Stages

1

Create a test policy to define the generated tests for the generated test suite, as required.

- Create an IP path test policy. See 13.6 “To create an IP path test policy” (p. 250) for more information.
- Create an LSP test policy. See 13.7 “To create an LSP test policy” (p. 254) for more information.
- Create a P2MP LSP test policy. See 13.8 “To create a P2MP LSP test policy” (p. 257) for more information.

2

Create an OAM test execution policy to define the parameters that control the execution of the OAM tests. See 13.9 “To configure an OAM test execution policy” (p. 261) for more information.

3

Associate the test policy with a path monitor. See Chapter 8, “Path and prefix monitoring” .

4

Manually run an IP path monitor or LSP path monitor test. See 13.10 “To manually run an OAM diagnostic on an IP, LSP, or P2MP path monitor” (p. 262) for more information.

5

Monitor the diagnostic results from the tests and the alarm list for indications of rising or falling thresholds. See 13.10 “To manually run an OAM diagnostic on an IP, LSP, or P2MP path monitor” (p. 262) for more information.

6

Highlight the OAM diagnostic results on a topology map.

- Highlight the results of a multicast trace OAM diagnostic on a topology map. See 13.11 “To view OAM test results of an IP, LSP, or P2MP path monitor” (p. 263) for more information.

- Highlight the results of a multicast trace OAM diagnostic on a topology map. See 13.12 “To highlight the results of a multicast trace OAM diagnostic on a topology map” (p. 264) for more information.
- Highlight the results of an LSP trace OAM diagnostic on a topology map. See 13.13 “To highlight the results of an LSP trace OAM diagnostic on a topology map” (p. 265) for more information.
- Highlight the results of an ICMP route trace OAM diagnostic on a topology map. See 13.14 “To highlight the results of an ICMP route trace OAM diagnostic on a topology map” (p. 266) for more information.
- Highlight the results of an OAM trace diagnostic on a topology map from the NFM-P Service Test Manager. See 13.15 “To highlight the results of an OAM trace diagnostic on a topology map from the NFM-P Service Test Manager” (p. 267) for more information.
- Highlight the results of a multicast trace diagnostic on a topology map from the NFM-P Service Test Manager. See 13.16 “To highlight the results of a multicast trace diagnostic on a topology map from the NFM-P Service Test Manager” (p. 268) for more information.

13.6 To create an IP path test policy

13.6.1 General information

The number of test results that are maintained by the CPAM is configured separately from the number of path records. The CPAM deletes historical results and historical path records at different intervals. Consider the following when you create an IP path test policy and view associated path records or results:

- A test result that is associated with a path record may be deleted before the path record is deleted.
- A path record may be deleted before the associated test result.
- Both the path record and the test result may be deleted simultaneously.

13.6.2 Steps

1

Choose Tools→Service Test Manager (STM) from the NFM-P main menu. The Service Test Manager form opens.

2

Click on the Create button.

3

Choose Create Test Policy from the Create contextual menu. The Test Policy (Create) form opens.

4

Set the Entity Type parameter to IP Path.

5

Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Strategy
- Ignore Probe Results

6

Click on the Test Definitions tab button.

7

Click on the Add button to add a test definition to the test policy. A menu appears.

8

Choose one of the following from the contextual menu:

- ICMP→Add ICMP Ping
- ICMP→Add ICMP Trace

The ICMP *test_type* Definition (Create) form opens with the General tab displayed.

9

Configure the parameters:

- Name
- Description
- Administrative State
- NE Persistent
- Router Instance

Note: The NE Persistent parameter must be disabled in order to perform auto-OAM operations.

10

Click on the Test Parameters tab button.

11

Perform one of the following:

a. If you are creating an ICMP Ping Definition, configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Rapid
- Time To Live
- Data Pattern
- Positional Data Pattern
- DiffServ Field
- Bypass Routing
- Do Not Fragment

b. If you are creating an ICMP Trace Definition, configure the parameters:
   - Number of Test Probes
   - Probe Interval (seconds)
   - Probe Timeout (seconds)
   - DiffServ Field
   - Time To Wait (milliseconds)

12

Click on the Results Configuration tab button.

13

Perform one of the following:

a. If you are creating an ICMP Ping Definition, configure the parameters:
   - Probe History Size (rows)
   - Test Failure Threshold
   - Probe Failure Threshold
   - Trap Generation

b. If you are creating an ICMP Trace Definition, configure the parameters:
   - Probe History Size (rows)
   - Maximum Failures
   - Trap Generation

14

Click on the Threshold Alarms tab button to configure threshold crossing alarms for test policies, test definitions, and assurance tests. An alarm is raised when a threshold is crossed, either because the value rose above or fell below the configured level. Configuring threshold crossing alarms on a test definition within the test policy creates a threshold definition that applies to generated tests.

15

Click on the Create button. The Threshold Event Definition (Create) form opens.

16

Perform the following:

1. Configure the parameters.
   - Type
   - Generate Alarm on Rising Threshold
   - Clear Alarm on Falling Threshold
   - Update Test Result Status
   - Include Falling Threshold
2. Click on the Rising Threshold tab.
3. Configure the Threshold Value parameter.
4. Click on the Falling Threshold tab.

   Note:

   The Falling Threshold tab can be accessed only when the Include Falling Threshold parameter is enabled on the General tab of the Threshold Event Definition, (Create) form.
5. Configure the Threshold Value parameter.
6. Click on the OK button. The Threshold Event Definition, (Create) form closes and a dialog box appears.
7. Click on the OK button. The dialog box closes and the test appears on the list.
8. Repeat 1 to 7 to configure threshold events on additional tests.

17

Perform Step 6 to Step 9 to add additional OAM tests to the policy.

18

Click on the OK button. The ICMP *test_type* Definition (Create) form closes and a dialog box appears.

19

Click on the OK button. The dialog box closes and the test definition appears in the list of test definitions.

20

Repeat Step 8 to Step 19 .

21

Click on the OK button. The Test Policy (Create) form closes.

22

Close the Service Test Manager form.

Note: To associate a test policy with an IP path monitor, LSP path monitor, or P2MP path monitor, see Chapter 8, “Path and prefix monitoring” .

End of steps

13.7 To create an LSP test policy

13.7.1 General information

The number of test results that are maintained by the CPAM is configured separately from the number of path records. The CPAM deletes historical results and historical path records at different intervals. Consider the following when you create an LSP path test policy and view associated path records or results:

- A test result that is associated with a path record may be deleted before the path record is deleted.
- A path record may be deleted before the associated test result.
- Both the path record and the test result may be deleted simultaneously.

13.7.2 Steps

1

Choose Tools→Service Test Manager (STM) from the NFM-P main menu. The Service Test Manager form opens.

2

Click on the Create button.

3

Choose Create Test Policy from the Create contextual menu. The Test Policy (Create) form opens.

4

Set the Entity Type parameter to LSP.

5

Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Strategy
- Ignore Probe Results

6

Click on the Test Definitions tab button.

7

Click on the Add button to add a test definition to the test policy. A menu appears.

8

Choose one of the following from the contextual menu:

- MPLS→Add LSP Ping
- MPLS→Add LSP Trace

The LSP *test_type* Definition (Create) form opens with the General tab displayed.

9

Configure the parameters:

- Name
- Description
- Administrative State
- NE Persistent
- Target Type

10

Click on the Test Parameters tab button.

11

Perform one of the following:

a. If you are creating an LSP Ping Definition, configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Time To Live
- Forwarding Class
- Forwarding Profile

b. If you are creating an LSP Trace Definition, configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Initial Time to Live
- Maximum Time to Live
- Forwarding Class
- Forwarding Profile

12

Click on the Results Configuration tab button.

13

Perform one of the following:

a. If you are creating an LSP Ping Definition, configure the parameters:
   - Probe History Size (rows)
   - Test Failure Threshold

- Probe Failure Threshold
- Trap Generation

b. If you are creating an LSP Trace Definition, configure the parameters:
   - Probe History Size (rows)
   - Maximum Failures
   - Trap Generation

14

Click on the Threshold Alarms tab button.

15

Click on the Create button. The Threshold Event Definition (Create) form opens.

16

Click on the Threshold Alarms tab button to configure threshold crossing alarms for test policies, test definitions, and assurance tests. An alarm is raised when a threshold is crossed, either because the value rose above or fell below the configured level. Configuring threshold crossing alarms on a test definition within the test policy creates a threshold definition that applies to generated tests.

17

Click on the Create button. The Threshold Event Definition (Create) form opens.

18

Perform the following:

1. Configure the parameters.
   - Type
   - Generate Alarm on Rising Threshold
   - Clear Alarm on Falling Threshold
   - Update Test Result Status
   - Include Falling Threshold
2. Click on the Rising Threshold tab.
3. Configure the Threshold Value parameter.
4. Click on the Falling Threshold tab.

   Note:

   The Falling Threshold tab can be accessed only when the Include Falling Threshold parameter is enabled on the General tab of the Threshold Event Definition, (Create) form.
5. Configure the Threshold Value parameter.
6. Click on the OK button. The Threshold Event Definition, (Create) form closes and a dialog box appears.
7. Click on the OK button. The dialog box closes and the test appears on the list.

8. Repeat 1 to 7 to configure threshold events on additional tests.

19

Perform Step 6 to Step 9 to add additional OAM tests to the policy.

20

Click on the OK button. The LSP *test_type* Definition (Create) form closes and a dialog box appears.

21

Click on the OK button. The dialog box closes and the test definition appears in the list of test definitions.

22

Repeat Step 8 to Step 21 .

23

Click on the OK button. The Test Policy (Create) form closes.

24

Close the Service Test Manager form.

Note: To associate a test policy with an IP path monitor, LSP path monitor, or P2MP LSP path monitor, see Chapter 8, “Path and prefix monitoring” .

END OF STEPS

13.8 To create a P2MP LSP test policy

13.8.1 General information

The number of test results that are maintained by the CPAM is configured separately from the number of path records. The CPAM deletes historical results and historical path records at different intervals. Consider the following when you create a P2MP LSP path test policy and view associated path records or results:

- A test result that is associated with a path record may be deleted before the path record is deleted.
- A path record may be deleted before the associated test result.
- Both the path record and the test result may be deleted simultaneously.

13.8.2 Steps

1

Choose Tools→Service Test Manager (STM) from the NFM-P main menu. The Service Test Manager form opens.

2

Click on the Create button.

3

Choose Create Test Policy from the Create contextual menu. The Test Policy (Create) form opens.

4

Set the Entity Type parameter to P2MP LSP.

5

Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Strategy
- Ignore Probe Results

6

Click on the Test Definitions tab button.

7

Click on the Add button to add a test definition to the test policy. A menu appears.

8

Choose one of the following from the contextual menu:

- MPLS→Add P2MP LSP Ping
- MPLS→Add P2MP LSP Trace

The P2MP LSP *test_type* Definition (Create) form opens with the General tab displayed.

9

Configure the parameters:

- Name
- Description
- Administrative State
- NE Persistent

- Target Type

10

Click on the Test Parameters tab button.

11

Perform one of the following:

a. If you are creating a P2MP LSP Ping Definition, configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Time To Live
- Forwarding Class
- Forwarding Profile

b. If you are creating a P2MP LSP Trace Definition, configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Initial Time to Live
- Maximum Time to Live
- Forwarding Class
- Forwarding Profile

12

Click on the Results Configuration tab button.

13

Perform one of the following:

a. If you are creating a P2MP LSP Ping Definition, configure the parameters:
   - Probe History Size (rows)
   - Test Failure Threshold
   - Probe Failure Threshold
   - Trap Generation

b. If you are creating a P2MP LSP Trace Definition, configure the parameters:
   - Probe History Size (rows)
   - Maximum Failures
   - Trap Generation

14

Click on the Threshold Alarms tab button.

15

Click on the Create button. The Threshold Event Definition (Create) form opens.

16

Click on the Threshold Alarms tab button to configure threshold crossing alarms for test policies, test definitions, and assurance tests. An alarm is raised when a threshold is crossed, either because the value rose above or fell below the configured level. Configuring threshold crossing alarms on a test definition within the test policy creates a threshold definition that applies to generated tests.

17

Click on the Create button. The Threshold Event Definition (Create) form opens.

18

Perform the following:

1. Configure the parameters.
   - Type
   - Generate Alarm on Rising Threshold
   - Clear Alarm on Falling Threshold
   - Update Test Result Status
   - Include Falling Threshold
2. Click on the Rising Threshold tab.
3. Configure the Threshold Value parameter.
4. Click on the Falling Threshold tab.

   Note:

   The Falling Threshold tab can be accessed only when the Include Falling Threshold parameter is enabled on the General tab of the Threshold Event Definition, (Create) form.
5. Configure the Threshold Value parameter.
6. Click on the OK button. The Threshold Event Definition, (Create) form closes and a dialog box appears.
7. Click on the OK button. The dialog box closes and the test appears on the list.
8. Repeat 1 to 7 to configure threshold events on additional tests.

19

Perform Step 6 to Step 9 to add additional OAM tests to the policy.

20

Click on the OK button. The P2MP LSP *test_type* Definition (Create) form closes and a dialog box appears.

21

Click on the OK button. The dialog box closes and the test definition appears in the list of test definitions.

22

Repeat Step 8 to Step 21 .

23

Click on the OK button. The Test Policy (Create) form closes.

24

Close the Service Test Manager form.

Note: To associate a test policy with an IP path monitor, LSP path monitor, or P2MP LSP path monitor, see Chapter 8, “Path and prefix monitoring” .

End of steps

13.9 To configure an OAM test execution policy

13.9.1 Introduction

An OAM execution policy specifies a hold time and priority for the Auto OAM test (the STM Policy) assigned to a path monitor.

The hold time determines how quickly a test is performed after a path reroutes. The CPAM delays test execution for the configured hold time to prevent multiple tests from generating while paths are unstable or rerouting repeatedly.

The priority level for the associated path monitor helps to determine which paths are first to undergo a test. The CPAM feature set uses an internal mechanism to manage Auto OAM test generation. The configurable Priority parameter allows some user control over which tests are performed first, and for which paths. For example, a user may prioritize tests on IP paths over LSP paths.

OAM execution policies are assigned to path monitors during path monitor configuration. If no execution policy is assigned, default values are used.

13.9.2 Steps

1

Choose Tools→Route Analysis→Path and Prefix Monitoring from the NFM-P main menu. The Path and Prefix Monitoring form opens.

2

Choose OAM Execution Policy (Monitored Path) in the object drop down.

3

Click Search, choose a policy in the list, and click Properties, or click Create and choose Execution Policy from the menu. The OAM Execution Policy (Create|Edit) form opens.

4

Configure the required parameters.

For the Priority parameter, lower numerical values indicate higher priority. For example, a value of 0 establishes high priority; a value of 7 establishes low priority.

5

Save your changes and close the forms.

END OF STEPS

13.10 To manually run an OAM diagnostic on an IP, LSP, or P2MP path monitor

13.10.1 General information

The CPAM automatically runs IP path monitor and LSP path monitor tests whenever there is a path reroute or according to the associated execution policy.

Perform this procedure to manually run an IP path monitor or LSP path monitor test.

13.10.2 Steps

1

Choose Tools→Route Analysis→Path Monitoring from the NFM-P main menu. The Path Monitoring form opens.

2

Choose one of the following from the object menu and click on the Search button.

- IP Path Monitor (Monitored Path)
- LSP Path Monitor (Monitored Path)
- P2MP LSP Path Monitor (Monitored Path)

3

Choose an entry and click on the Properties button. The *IP/LSP/P2MP LSP* Path Monitor (Edit) form opens with the General tab displayed.

4

Click on the Run OAM button. A dialog box appears.

5

Click on the OK button. The dialog box closes.

6

See 13.11 “To view OAM test results of an IP, LSP, or P2MP path monitor” (p. 262) to view the test results.

END OF STEPS

13.11 To view OAM test results of an IP, LSP, or P2MP path monitor

13.11.1 Steps

1

Choose Tools→Route Analysis→Path Monitoring from the NFM-P main menu. The Path Monitoring form opens.

2

Choose one of the following from the object menu and click on the Search button.

- IP Path Monitor (Monitored Path)
- LSP Path Monitor (Monitored Path)
- P2MP LSP Path Monitor (Monitored Path)

3

Choose an entry and click on the Properties button. The *IP/LSP/P2MP LSP* Path Monitor (Edit) form opens with the General tab displayed.

4

Click on the Auto OAM tab button. The General tab is displayed.

5

Click on the Results tab button. A list of results appears.

6

Choose an entry and click on the Properties button. The Tested Entity Result (Edit) form opens with the General tab displayed.

7

View information about the execution status.

8

Click on the Results tab button.

9

Click on the Search button.

10

Choose an entry and click on the Properties button. The *Test_type* Result - Result (Edit) form opens with the General tab displayed.

11

View the test result details. Click on the tab buttons for information about the test.

12

Close the *Test_type* Result - Result (Edit) form. The Tested Entity Result (Edit) form reappears.

13

Click on the View Associated Record button to view the IP, LSP, or P2MP LSP path record associated with the test result, if necessary. The *IP/LSP/P2MP LSP* Path Record (Edit) form appears with the General tab displayed.

14

Close the *IP/LSP* Path Record (Edit) form.

15

Close the Tested Entity Result (Edit) form.

16

Close the *IP/LSP* Path Monitor (Edit) form.

17

Close the Path Monitoring form.

END OF STEPS

13.12 To highlight the results of a multicast trace OAM diagnostic on a topology map

13.12.1 Steps

1

Perform the following using the NFM-P.

For tests on IP and LSP path monitors, see 13.6 “To create an IP path test policy” (p. 250) and 13.7 “To create an LSP test policy” (p. 254) .

1. Create a test policy.
2. Create a test suite.
3. Execute the test suite.

2

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate IGP topology map opens.

3

Right-click on the map and choose Highlight Multicast Trace from the contextual menu. The Find Multicast Trace Result form opens.

4

Click on the Search button. A list of multicast trace results appears.

5

Choose an entry and click on the OK button. The Find Multicast Trace Results form closes and the results are highlighted on the topology map.

6

Perform 7.32 “To manage active highlights on a topology map” (p. 123) to manage highlights on the topology map.

END OF STEPS

13.13 To highlight the results of an LSP trace OAM diagnostic on a topology map

13.13.1 Steps

1

Perform the following using the NFM-P.

1. Create a test policy.
2. Create a test suite.
3. Execute the test suite.

2

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate IGP topology map opens.

3

Right-click on the map and choose Highlight LSP Trace from the contextual menu. The Find LSP Trace Result form opens.

4

Click on the Search button. A list of LSP trace results appears.

5

Choose an entry and click on the OK button. The Find LSP Trace Results form closes and the results are highlighted on the topology map.

6

Perform 7.32 “To manage active highlights on a topology map” (p. 123) to manage highlights on the topology map.

END OF STEPS

13.14 To highlight the results of an ICMP route trace OAM diagnostic on a topology map

13.14.1 Steps

1

Perform the following using the NFM-P.

1. Create a test policy.
2. Create a test suite.
3. Execute the test suite.

2

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate IGP topology map opens.

3

Right-click on the map and choose Highlight ICMP Route Trace from the contextual menu. The Find ICMP Route Trace Result form opens.

4

Click on the Search button. A list of ICMP route trace results appears.

5

Choose an entry and click on the OK button. The Find ICMP Route Trace Results form closes and the results are highlighted on the topology map.

6

Perform 7.32 “To manage active highlights on a topology map” (p. 123) to manage highlights on the topology map.

END OF STEPS

13.15 To highlight the results of an OAM trace diagnostic on a topology map from the NFM-P Service Test Manager

13.15.1 Steps

1

Choose Tools→Service Test Manager (STM) from the NFM-P main menu. The Manage Tests form opens.

2

Choose Test Suite (Assurance) from the object drop-down menu.

3

Specify a filter for the search, if required.

4

Click on the Search button.

5

Choose an entry and click on the Properties button. The Test Suite (Edit) form opens with the General tab displayed.

6

Click on the Results tab. The Test Suite (Edit) Filter form opens.

7

Specify a filter for the search and click on the OK button. The Test Suite (Edit) Filter form closes.

8

Select a result entry.

9

Click on the Navigate button to select a topology map view.

10

The appropriate topology map appears showing the network objects and the highlighted results.

11

To remove the highlights, right-click on the map area and choose Clear from the contextual menu.

12

Close the topology map view.

13

Close the Test Suite (Edit) form.

14

Close the Manage Tests form.

END OF STEPS

13.16 To highlight the results of a multicast trace diagnostic on a topology map from the NFM-P Service Test Manager

13.16.1 Steps

1

Create a router test policy, as described in the *NSP NFM-P Classic Management User Guide*, with the following attributes:

- multicast group
- test parameters

2

Create a test suite, as described in the *NSP NFM-P Classic Management User Guide*.

3

Specify the routers that receive multicast traffic for the group.

4

Execute the test suite.

5

Perform 13.15 “To highlight the results of an OAM trace diagnostic on a topology map from the NFM-P Service Test Manager” (p. 267) to view the results of the multicast trace from a router.

END OF STEPS

14 Root cause analysis

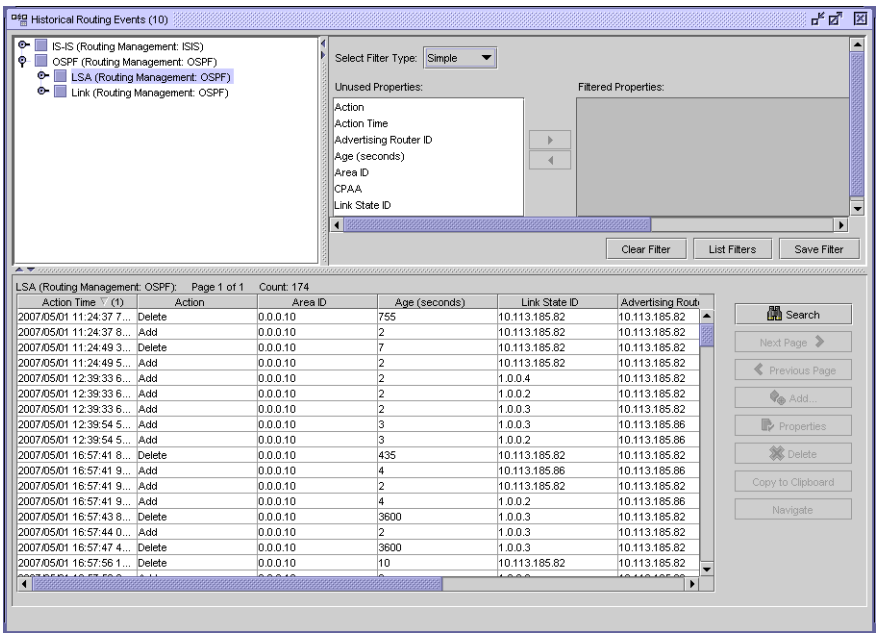
14.1 Root cause analysis overview

14.1.1 Introduction

You can use the CPAM as a tool for determining the root cause of a problem, such as a service outage or service degradation. For example, you can view the time of a service outage to determine how the network was behaving at that time. The CPAM records IGP network events—such as router and network LSAs—in the database.

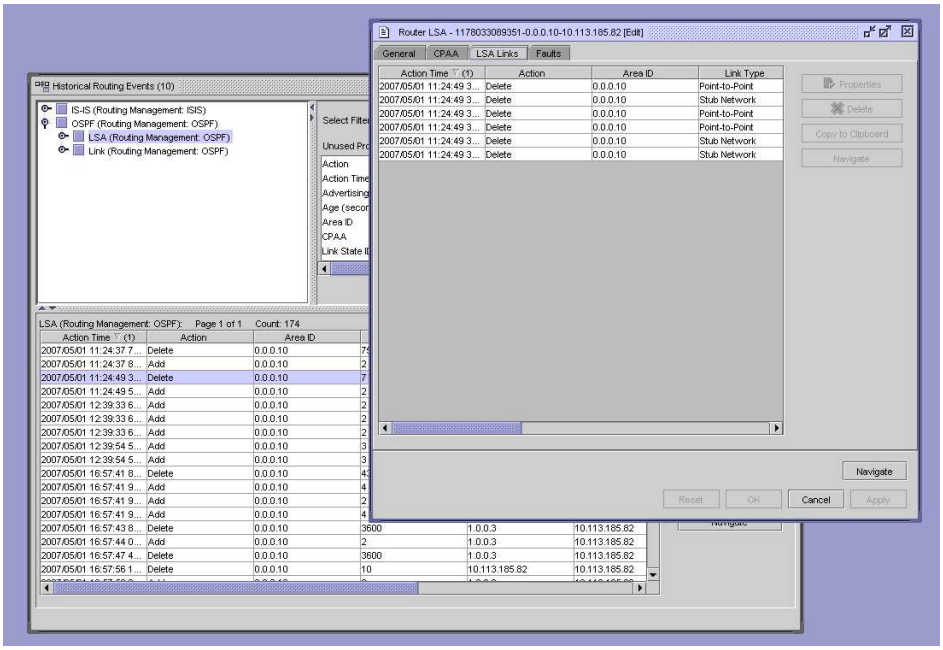
You can specify whether the events are recorded on each CPAA on a per-CPAA basis, and on a protocol-by-protocol basis (OSPF, OSPF-TE, ISIS-TE). You can use size constraint policies to control the number of events stored in the database. You can export historical data using the XML API or the NFM-P GUI. The following figure displays the CPAM search form for captured events.

Figure 14-1 Browse network-level protocol objects



The following figure shows the drill-down of captured events into detailed LSA information.

Figure 14-2 Browse network-level protocol events



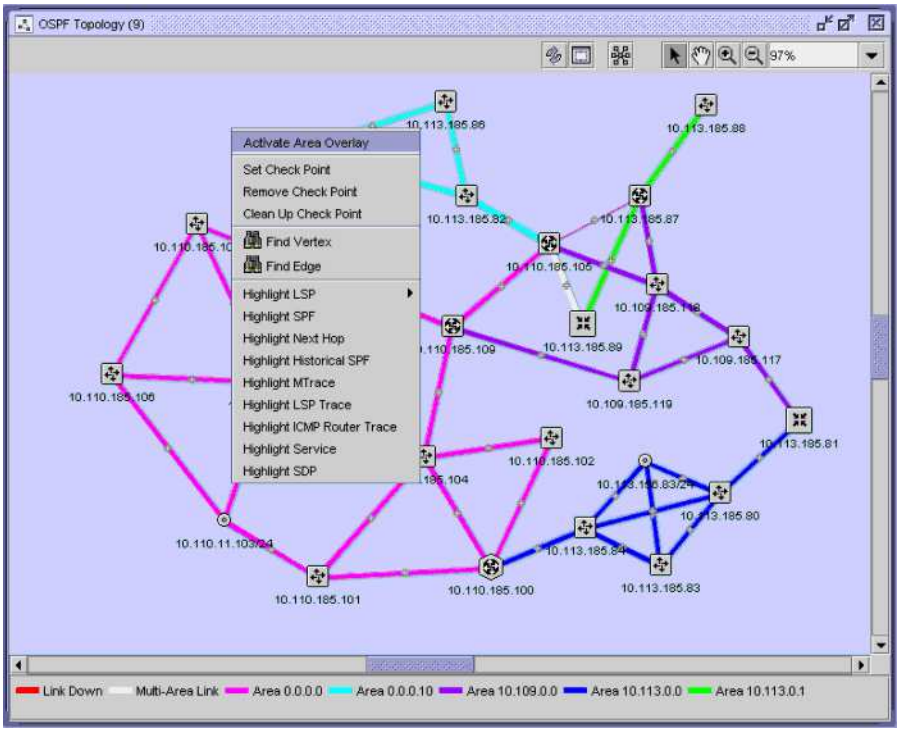
The recording of IGP router events into a database allows you to filter and analyze historical data to determine if any significant routing events occurred. The CPAM allows you to highlight routers and links on the topology map that were affected by a router event. All window entries, such as LSA, follow the standard NFM-P filtering and sorting functionality.

Note: See Chapter 8, “Path and prefix monitoring” for more information about configuring size constraint policies.

You must enable the Keep Event History parameter on the CPAA configuration form to save historical events. See 10.8 “To deploy a CPAA to monitor a BGP AS” (p. 199) for information.

You can select map objects that are affected by specific protocol events. The following figure shows the Find Vertex and Find Edge contextual menu options that you can use to search for map objects.

Figure 14-3 Find Vertex and Find Edge menu options

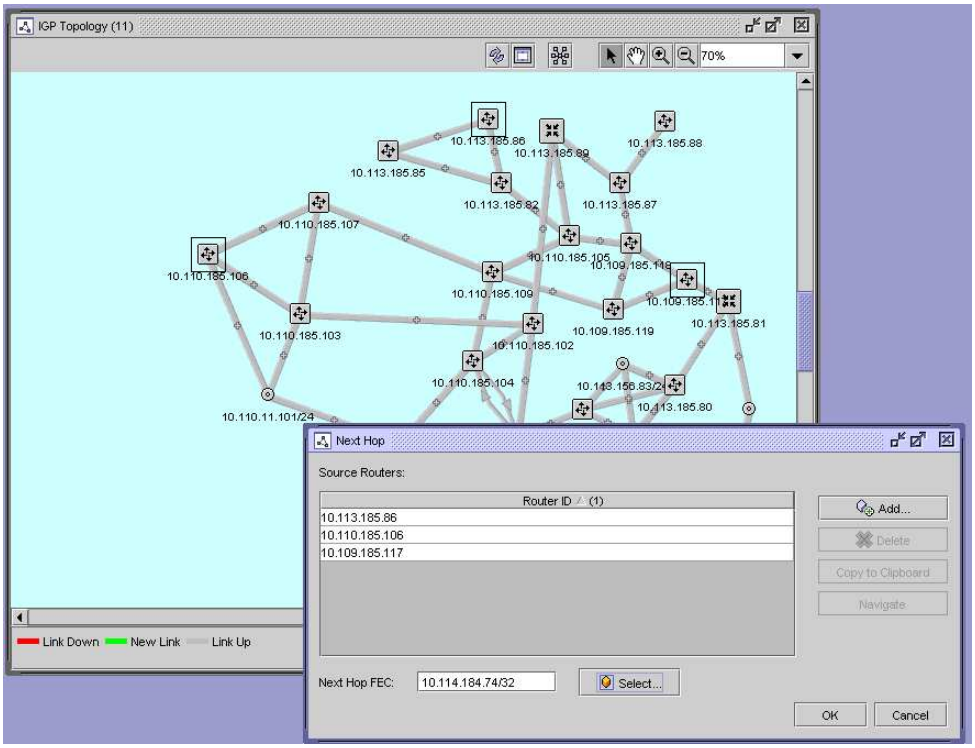


14.1.2 Next hop FEC overlay

You can view the next hop for a FEC from a set of routers that use the CPAM. By typing in a next hop prefix and selecting a group of routers, the next hops to a FEC are highlighted with arrows on the appropriate topology map. The next hop view can be used to search for suspicious routing of an address in the network. ECMP for next hop FEC overlay allows more than one link to be highlighted from a router. Routers that do not have a next hop for a FEC are displayed in an error dialog.

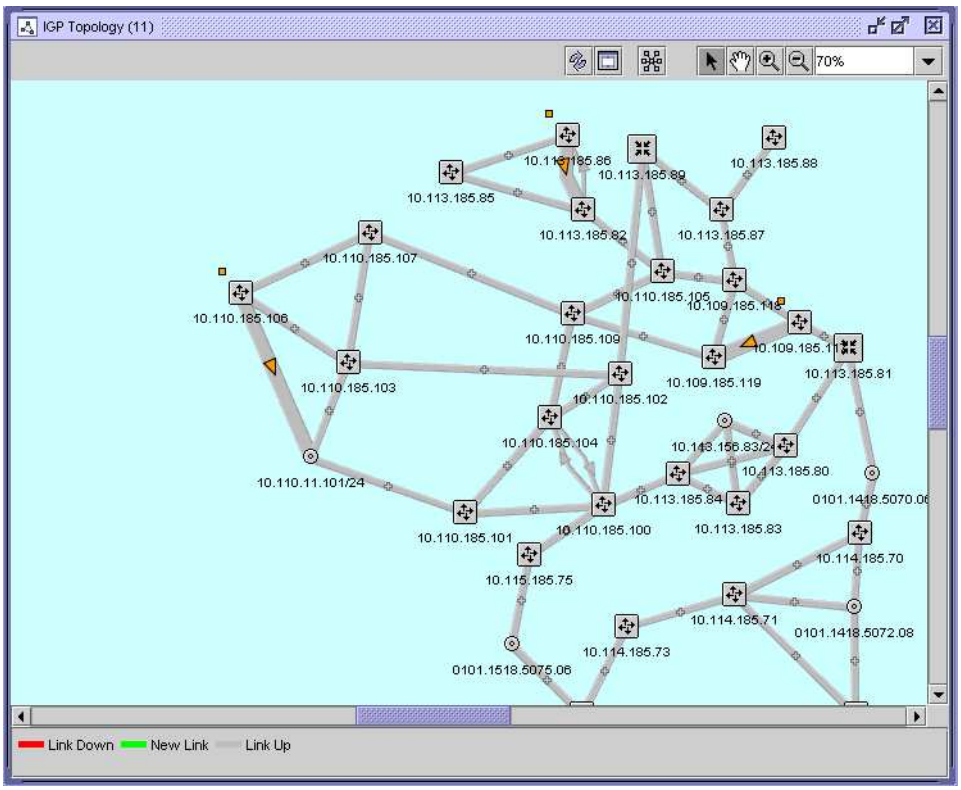
The following figure shows the next hop FEC configuration form.

Figure 14-4 Next hop FEC overlay configuration



The following figure shows the next hop FEC overlay results on the topology map.

Figure 14-5 Next hop FEC overlay results



14.2 Workflow for root cause analysis

14.2.1 Stages

1

Determine the map type you need to view:

- maps that show IGP topology
- maps that show protocol-specific topologies

2

Configure next hop highlighting to search for suspicious routing of an address in the network. See 14.3 “To configure next hop highlighting” (p. 274) for more information.

3

Configure IP path and LSP monitoring, if required. See Chapter 8, “Path and prefix monitoring” for more information.

4

Highlight historical records, if required. See Chapter 8, “Path and prefix monitoring” for more information.

5

Configure size constraint policies to control the number of events stored in the database. See Chapter 8, “Path and prefix monitoring” for more information.

14.3 To configure next hop highlighting

14.3.1 Steps

1

Choose Tools→Route Analysis→*Topology_type*→*IGP_Administrative_Domain* from the NFM-P main menu.

The appropriate topology map appears showing the network objects.

2

Right-click on the map and choose Highlight Next Hop from the contextual menu. The Next Hop form opens.

3

Click on the Add button. The Select Source Routers for Next Hop form opens.

4

Specify a filter for the search and click on the Search button. A list of routers appears.

5

Select a router and click on the OK button. The Select Source Routers for Next Hop form closes.

6

Click on the Select button next to the Next Hop FEC parameter. The Select Next Hop FEC form opens.

7

Choose an icon from the object drop-down menu.

8

Specify a filter for the search, if required, and click on the Search button.

9

Choose an entry and click on the OK button. The Select Next Hop FEC form closes.

10

Click on the OK button. The Next Hop form closes.

11

Perform 7.32 “To manage active highlights on a topology map” (p. 123) to manage highlights on the topology map.

END OF STEPS

15 RCA audit policies

15.1 RCA audit policies overview

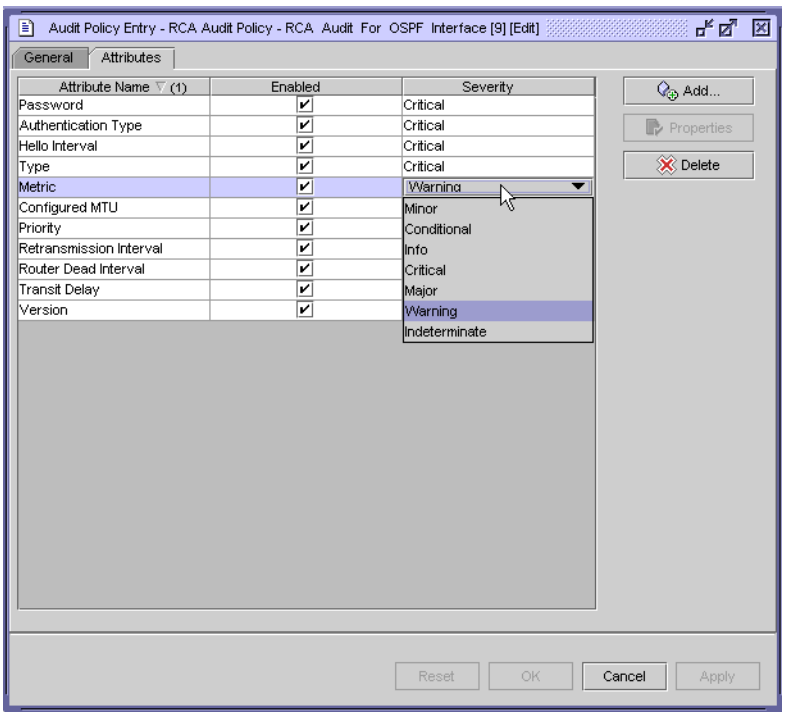
15.1.1 Introduction

The CPAM allows you to perform on-demand verifications of the IP/MPLS configuration of ISIS and OSPF routing protocols on NFM-P-managed NEs. RCA audit policies identify problems or errors in protocol-related and control plane configurations. These configuration problems, if not discovered in a timely manner, can have significant effects on higher layers, such as MPLS and VPN.

Note: An NFM-P user that is assigned the Administrator or RCA Verification scope of command role can create, modify, and execute all of the RCA audit policies. The results of an RCA audit are associated with the object, not the user.

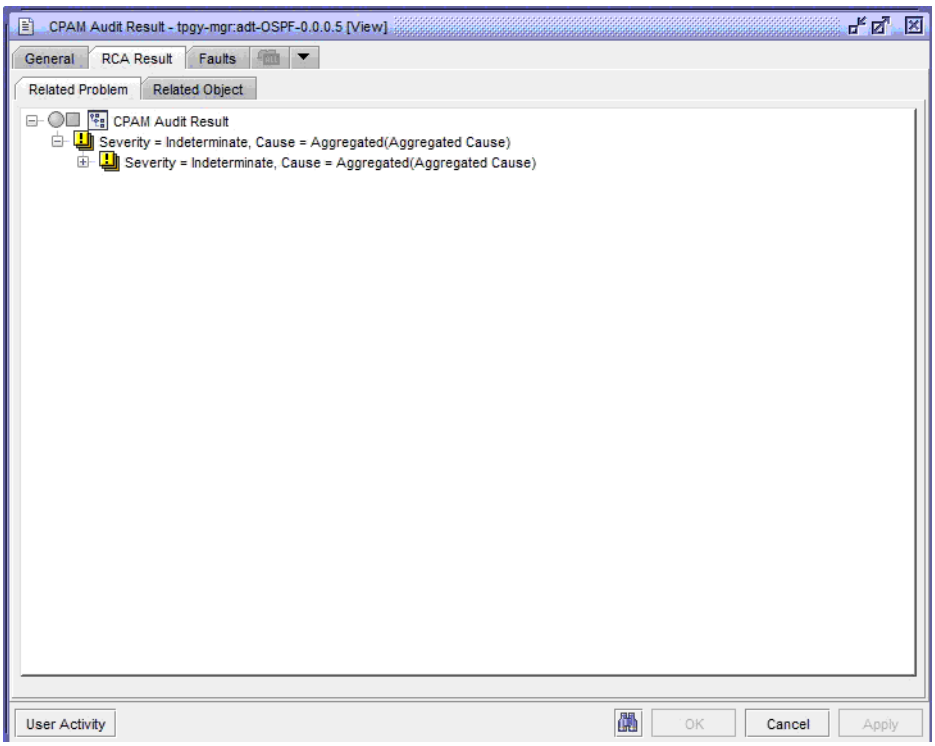
You can create RCA audit policies for IGP administrative domains to verify the configuration of network objects on NFM-P-managed routers. For each audit policy that you create, you can specify one or more policy entries that define the scope of configuration that is verified by the audit and the severity of the related problem, as displayed in the figure below. For example, an RCA audit policy on an OSPF interface verifies the configuration of several default attributes, such as the configured MTU and Hello interval. A problem with the specified severity is raised against the IGP administration domain for ISIS misconfigurations, the OSPF area for OSPF misconfigurations, and the ISIS or OSPF interface for interface misconfigurations, and so on, depending on the policy entry.

Figure 15-1 Audit policy entry form—Attribute and problem severity



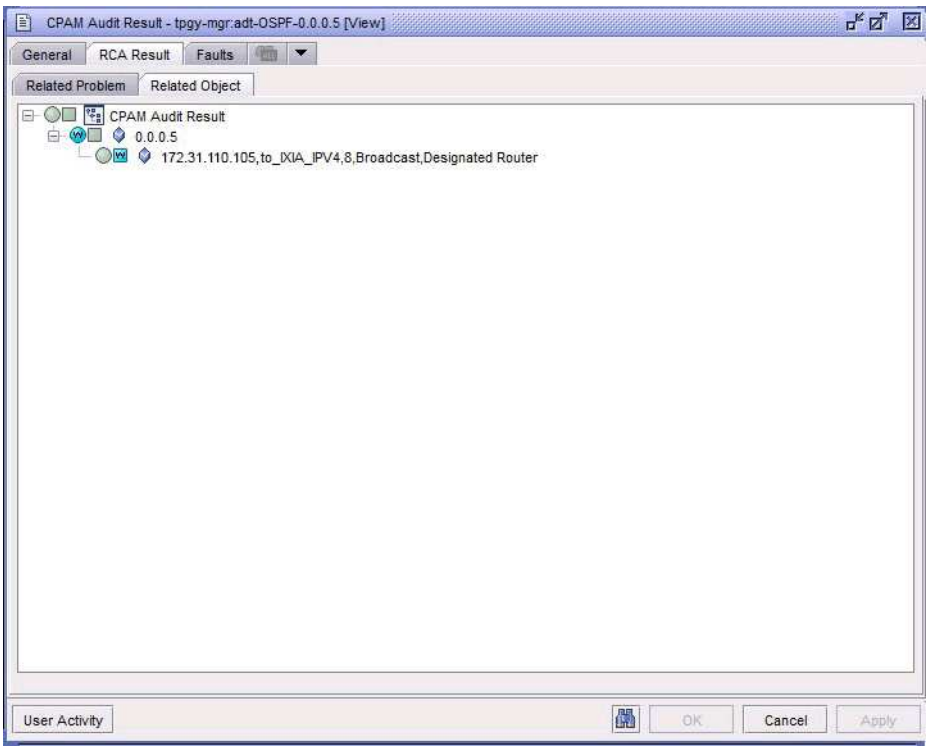
The results of the verification are displayed in two components trees: the problem tree and the object tree. You can expand the problem tree to view the problem type and other objects affected by the same problem, as displayed in the following figure:

Figure 15-2 RCA audit—problem tree



You can expand the object tree to view all of the problems that are associated with the selected object, as displayed in the figure below. You can also view RCA audit results on the properties form of an OSPF or ISIS interface or routing instance.

Figure 15-3 RCA audit—object tree



In addition to the attributes that you specify in an RCA audit policy, the CPAM verifies the following for each protocol:

- OSPF:
  - the administrative state of the corresponding OSPF router interface
  - the MTU of the OSPF interface with the MTU of the physical port
  - verifies the far-end if the interface is not passive
- ISIS:
  - the administrative state of the corresponding ISIS router interface
  - whether the ISIS instance is L1 and the ISIS interface is L2
  - whether the ISIS instance is L2 and the ISIS interface is L1
  - whether the ISIS instance is L1 (L1/L2) and the ISIS interface is L2 (I1/L2) and missing an ISIS area
  - whether the ISIS interface is L1 and (L1/L2) and the far-end ISIS interface is L1 (L1/L2) and missing a common area
  - whether the ISIS instance is L1 and the far-end ISIS interface is L2
  - whether the ISIS instance is L2 and the far-end ISIS interface is L1

15.2 Workflow for RCA audit policies

15.2.1 Stages

1

Create an RCA audit policy to verify the IP/MPLS configuration of ISIS and OSPF routing protocols on NFM-P-managed NEs. Configure the attributes that are verified for each RCA audit policy entry. See 15.3 “To create an RCA audit policy” (p. 281) for more information.

2

Run the RCA audit policy on a specific object:

- Perform an RCA audit on an ISIS configuration in an IGP administrative domain. See 15.4 “To perform an RCA audit on an ISIS configuration in an IGP administrative domain” (p. 284) for more information.
- Perform an RCA audit on an OSPF area in an IGP administrative domain. See 15.5 “To perform an RCA audit on an OSPF area in an IGP administrative domain” (p. 285) for more information.

3

View the results of a completed RCA audit. See 15.6 “To view completed RCA audit results” (p. 286) for more information.

4

Highlight the results of a completed RCA audit on a topology map:

- Highlight an ISIS RCA audit result on a topology map. See 15.7 “To highlight the results of an OSPF RCA audit on a topology map” (p. 287) for more information.
- Perform an OSPF RCA audit result on a topology map. See 15.8 “To highlight the results of an ISIS RCA audit on a topology map” (p. 288) for more information.

15.3 To create an RCA audit policy

15.3.1 Steps

1

Perform one of the following:

a. To create any RCA audit policy, choose Policies→RCA Audits from the NFM-P main menu. The Network and Service Audits form opens.

b. To create an ISIS or OSPF RCA audit policy, choose Tools→Route Analysis→CPAM Audit Manager from the NFM-P main menu. The CPAM Audit Manager form opens.

2

Choose Audit Policy (RCA) from the object drop-down menu.

3

Click on the Create button. The Audit Policy (Create) form opens with the General tab displayed.

4

Configure the parameters:

- Auto-Assign ID
- ID
- Description

5

Click on the Select RCA Policy to run the audit button next to the Policy Type Description parameter. The RCA Policy form opens.

6

Select one of the following entries:

- RCA Audit ISIS
- RCA Audit OSPF

7

Click on the Apply button.

8

Click on the Entry tab button. Depending on the option you selected in Step 5 for the Policy Type Description parameter, a list of RCA audit policy entries appear.

The following are the RCA audit policy entries for an OSPF RCA audit:

- RCA Audit For Network Interface
- RCA Audit For OSPF Interface

The following are the RCA audit policy entries for an ISIS RCA audit:

- RCA Audit For ISIS Interface
- RCA Audit For ISIS Interface L1
- RCA Audit For ISIS Interface L2
- RCA Audit For ISIS Network Interface

9

Choose an entry and click on the Properties button. The Audit Policy Entry - RCA Audit Policy - *Network_Object* Audit (Edit) form opens with the General tab displayed.

10

Configure the Enabled parameter.

11

Click on the Attributes tab button. A list of default attributes for the network object is displayed.

12

Perform one of the following:

a. To configure default attributes, go to Step 13 .

b. To add a new attribute, go to Step 15 .

13

Enable or disable the RCA audit for each attribute by enabling or disabling the checkbox in the Enabled column.

14

Choose the problem severity for each attribute by clicking on the entry in the Severity column of the attribute. A contextual menu appears with the following options:

- Minor
- Conditional
- Info
- Critical
- Major
- Warning
- Indeterminate

15

Click on the Add button to add a new attribute. Otherwise, go to Step 18 . The Adding new Attribute(s) - *Network_Object* Audit form opens with a list of attributes.

16

Select one or more items in the list and click on the OK button. The Adding new Attribute(s) - *Network_Object* Audit form closes and the Audit Policy Entry - RCA Audit Policy - RCA Audit For *Network_Object* (Edit) form refreshes with the attribute information.

17

Perform Step 13 and Step 14 to configure the attributes, if necessary.

18

Click on the OK button. The Audit Policy Entry - RCA Audit Policy - *Network_Object* Audit (Edit) form closes.

19

Click on the OK button on the Audit Policy (Edit) form. A dialog box appears.

20

Click on the Yes button. The Audit Policy (Edit) form closes.

END OF STEPS

15.4 To perform an RCA audit on an ISIS configuration in an IGP administrative domain

15.4.1 Steps

1

Choose Tools→Route Analysis→CPAM Audit Manager from the NFM-P main menu. The CPAM Audit Manager form opens.

2

Choose Audit Policy (RCA) from the object drop-down menu and click on the Search button.

3

Choose an RCA Audit ISIS entry from the list.

4

Perform one of the following:

a. Click on the RCA Audit button and choose All from the contextual menu. A dialog box appears. Go to Step 6 .

b. Click on the RCA Audit button and choose Backbone from the contextual menu. A dialog box appears. Go to Step 6 .

c. Click on the RCA Audit button and choose Area from the contextual menu. The Select ISIS Area form opens. Continue to Step 5 .

5

Choose up to five areas from the list and click on the OK button. A dialog box appears.

6

Click on the Yes button. The CPAM Audit form appears.

7

Choose the completed audit and click on the Details button. The CPAM Audit Result (View) form opens. See 15.6 “To view completed RCA audit results” (p. 286) for information about viewing completed RCA audit results.

8

Close the CPAM Audit Result (View) form.

9

Close the CPAM Audit Manager form.

End of steps

15.5 To perform an RCA audit on an OSPF area in an IGP administrative domain

15.5.1 Steps

1

Choose Tools→Route Analysis→Audit Manager from the NFM-P main menu. The Audit Manager form opens.

2

Choose Audit Policy (RCA) from the object drop-down menu and click on the Search button.

3

Choose an RCA Audit OSPF entry from the list.

4

Click on the RCA Audit and choose Area from the contextual menu. The Select OSPF Area form opens.

5

Choose up to five areas from the list and click on the OK button. A dialog box appears.

6

Click on the Yes button. The CPAM Audit form appears.

7

Choose the completed audit and click on the Details button. The CPAM Audit Result (View) form opens. See 15.6 “To view completed RCA audit results” (p. 286) for information about viewing completed RCA audit results.

8

Close the CPAM Audit Result (View) form.

9

Close the CPAM Audit Manager form.

End of steps

15.6 To view completed RCA audit results

15.6.1 Steps

1

Choose Tools→Route Analysis→CPAM Audit Manager from the NFM-P main menu. The IGP Network Data form opens.

2

Choose CPAM Audit Result (CPAM: topology) from the object drop-down menu and click on the Search button.

3

Choose a completed RCA audit and click on the Properties button. The CPAM Audit Result (View) form opens.

4

Choose the completed audit and click on the Details button. The CPAM Audit Result (View) form opens.

5

Click on the RCA Result tab.

6

Click on the Related Problem tab.

7

If required, expand aggregated problems to view underlying problems, or double-click on a non-aggregated problem to view additional information.

8

Click on the Related Objects tab.

9

If necessary, expand the audit result icon to view the related objects.

10

Double-click on an object in the list to view information about the problem.

11

Close the CPAM Audit Result (View) form.

12

Close the CPAM Audit Manager form.

END OF STEPS

15.7 To highlight the results of an OSPF RCA audit on a topology map

15.7.1 Steps

1

Choose Tools→Route Analysis→OSPF Topology from the NFM-P main menu.

The OSPF Topology map appears showing the network objects.

2

Right-click on the map and choose Highlight→RCA Results from the contextual menu. The RCA Results form opens.

3

Click on the Search button. A list of RCA results appears.

4

Choose an entry and click on the OK button. The RCA Results form closes and the results of the RCA audit are highlighted on the topology map.

5

To view the RCA audit results on an OSPF interface, perform the following:

1. Locate the highlighted OSPF link on the topology map.
2. Right-click on the link and choose Expand Group from the contextual menu to expand the group of links, if necessary.
3. Right-click on the link and choose Properties from the contextual menu. The OSPF Link (Edit) form opens with the General tab displayed.
4. Click on the Properties button in the Interface panel. The OSPF Interface (Edit) form opens with the General tab displayed.
5. Click on the RCA Result tab button. The Related Problem tab is displayed.
6. If necessary, expand the OSPF interface object to view the associated problems.
7. Double-click on a problem icon to view information about the problem. The Problem (Edit) form opens with the General tab displayed.
8. Click on the tab buttons to view information about the configuration.
9. Close the Problem (Edit) form.
10. Close the OSPF Interface (Edit) form.
11. Close the OSPF Link (Edit) form.

6

To view the RCA audit results on an OSPF area, perform the following:

1. Locate the highlighted OSPF router on the topology map.
2. Right-click on the router and choose Properties from the contextual menu. The Router (Edit) form opens with the General tab displayed.
3. Click on the Areas tab button.
4. Click on the Search button, if necessary. A list of areas appears.
5. Choose an entry and click on the Properties button. The Area (Edit) form opens with the General tab displayed.
6. Click on the RCA Result tab button. The Related Problem tab is displayed.
7. If necessary, expand the Area object to view the associated problems.
8. Double-click on a problem icon to view information about the problem. The Problem (Edit) form opens with the General tab displayed.
9. Click on the tab buttons to view information about the configuration.
10. Close the Problem (Edit) form.
11. Close the Area (Edit) form.
12. Close the Router (Edit) form.

7

Perform 7.32 “To manage active highlights on a topology map” (p. 123) to manage highlights on the topology map.

Note: RCA highlights on OSPF areas refer to interfaces on OSPF routers. If a router is also highlighted, an OSPF interface that is not displayed on the topology map may have a problem. When this occurs, the CPAM highlights only the router to indicate to the user that a problem exists with an interface on that router. This typically occurs when a CPAA discovers a router that is not managed by the NFM-P.

END OF STEPS

15.8 To highlight the results of an ISIS RCA audit on a topology map

15.8.1 Steps

1

Choose Tools→Route Analysis→ISIS Topology from the NFM-P main menu.

The ISIS Topology map appears showing the network objects.

2

Perform one of the following:

a. Right-click on the map and choose Highlight→RCA Results→All from the contextual menu. The RCA Results form opens.

b. Right-click on the map and choose Highlight→RCA Results→Backbone from the contextual menu. The RCA Results form opens.

c. Right-click on the map and choose Highlight→RCA Results→Area from the contextual menu. The RCA Results form opens.

3

Click on the Search button. A list of RCA results appears.

4

Choose an entry and click on the OK button. The RCA Results form closes and the results of the RCA audit are highlighted on the topology map.

5

To view the RCA audit results on an ISIS interface, perform the following:

1. Locate the highlighted ISIS link on the topology map.
2. Right-click on the link and choose Expand Group from the contextual menu to expand the group of links, if necessary.
3. Right-click on the link and choose Properties from the contextual menu. The ISIS Link (Edit) form opens with the General tab displayed.
4. Click on the Properties button in the Interface panel. The ISIS Interface (Edit) form opens with the General tab displayed.
5. Click on the RCA Result tab button. The Related Problem tab is displayed.
6. If necessary, expand the ISIS interface object to view the associated problems.
7. Double-click on a problem icon to view information about the problem. The Problem (Edit) form opens with the General tab displayed.
8. Click on the tab buttons to view information about the configuration.
9. Close the Problem (Edit) form.
10. Close the ISIS Interface (Edit) form.
11. Close the ISIS Link (Edit) form.

6

Perform 7.32 “To manage active highlights on a topology map” (p. 123) to manage highlights on the topology map.

END OF STEPS

16 Threshold reaching alarms

16.1 Threshold reaching alarms overview

16.1.1 Introduction

In addition to routing alarms generated by routers, there are threshold reaching alarms generated by the CPAA. The alarm generation process uses the routing data collected by the CPAA. The generated alarms are sent to the CPAM using a proprietary protocol over the TCP channel. The alarms are then available to CPAM XML API clients, in the same manner that alarms generated in the NFM-P are sent to XML API clients.

For threshold reaching alarms, you can use the NFM-P GUI to configure thresholds to suit your requirements. The alarms are listed by class and alarm name (with no spaces), and also use a long name for ease of reading and identification. The long name appears as the form name on the threshold configuration form. See 16.3 “To configure alarm thresholds” (p. 295).

The following table describes the CPAM threshold reaching alarms:

Table 16-1 CPAM threshold reaching alarms

Long name/Threshold configuration form name class.AlarmName	Index number	Description
BGP AS Path Length Per Monitored Prefix Threshold topology. BgpAsPathLenPerMonPrefThresholdReached	795	Raised when the AS path length for a monitored prefix reaches or exceeds the configured threshold. The alarm is cleared when the AS path length falls below the threshold.
BGP Redundancy Loss Per Monitored Prefix Threshold topology. BgpMonPrefRedundancyLossThresholdReached	796	Raised when number of next hops for a monitored prefix reaches or falls below the configured threshold. The alarm is cleared when the number of next hops exceeds the threshold.
BGP Monitor Prefix Flap Rate Threshold topology. BgpMonitorPrefixFlapRateThresholdReached	432	Raised when the rate of change—addition, withdrawal, or next hop change—for a BGP monitored prefix reaches or exceeds a predefined value. For BGP and MP-BGP.
BGP Packet Rate Threshold topology.BgpPktRateThresholdReached	431	Raised when the rate of update packets received by the CPAA reaches or exceeds a predefined value.
BGP Route Count Threshold topology.BgpRouteCountThresholdReached	428	Raised when the number of BGP routes received by a CPAA in a BGP AS for a specific next hop reaches or exceeds a predefined value.
BGP Route Flap Rate Threshold topology.BgpRouteFlapRateThresholdReached	430	Raised when the route withdrawal rate per second — an indication of route flapping — received for a specific next hop reaches or exceeds a predefined value.

Table 16-1 CPAM threshold reaching alarms (continued)

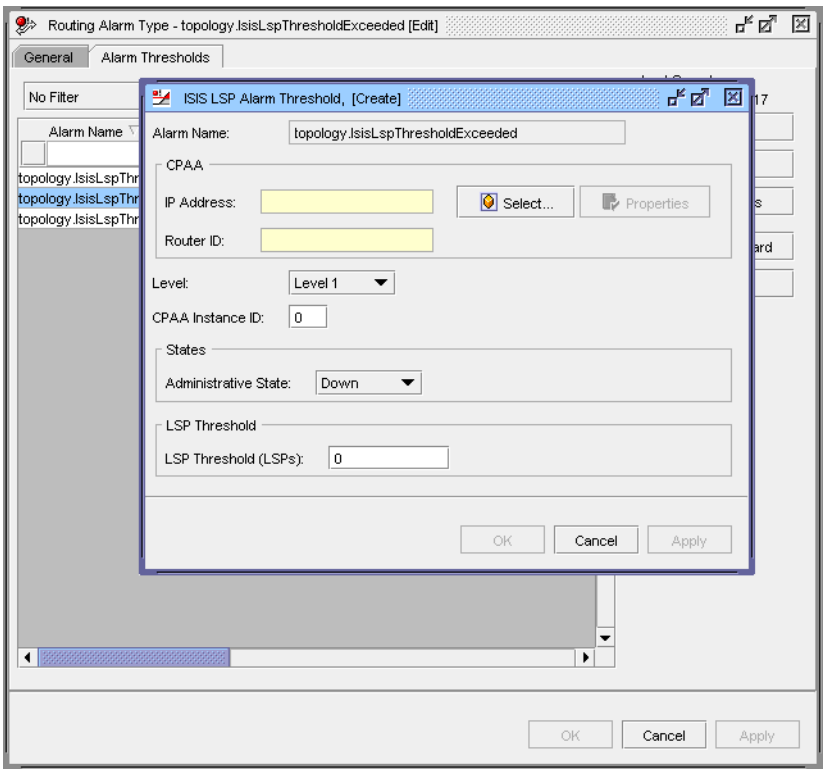
Long name/Threshold configuration form name class.AlarmName	Index number	Description
BGP Route High Watermark Per RT Threshold topology. BgpRouteHighWatermarkPerRTargetReached	433	Raised when the number of routes for an IP VPN route target reaches or exceeds a predefined value upper limit value.
BGP Route Low Watermark Per RT Threshold topology. BgpRouteLowWatermarkPerRTargetReached	434	Raised when the number of routes for an IP VPN route target reaches or falls below a predefined lower limit value.
BGP Route Rate Threshold topology.BgpRouteRateThresholdReached	429	Raised when the rate of the routes—both updates and withdrawal—received for a specific next hop reaches or exceeds a predefined value.
BGP Route Rate Per RT Threshold topology. BgpRouteRateThresholdPerRTargetReached	435	Raised when the rate of the routes—both updates and withdrawal— received for an IP VPN route target reaches or exceeds a predefined value.
BGP Route Change Per Next Hop Threshold topology. BgpRouteChangeThresholdPerNHopReached	601	Raised when the percentage of route changes for a next hop reaches or exceeds a predefined value.The range is 10% to 100%. For example, if the baseline is 10 000, and the percentage set by this threshold is 10%, an alarm is raised when the number of routes reaches 11 000 or drops to 9 000. When it drops down to 10 000, the alarm is cleared. If the number continues to rise or drop, no additional alarm or alarm history is added. A single baseline and threshold pair—10000 and 10%—is configured and used per next hop. If the number of routes is not the same as the predefined baseline, the alarm policy for that next hop is in effect only after the number exceeds or drops below the baseline.
BGP Route Change Per RT Threshold topology. BgpRouteChangeThresholdPerRTargetReached	600	Raised when the percentage of route changes for a IPv4 IP-VPN route target reaches or exceeds a predefined value. The range is 10% to 100%. For example, if the baseline is 10 000, and the percentage set by this threshold is 10%, an alarm is raised when the number reaches 11 000 or drops to 9 000. When it drops down to 10 000, the alarm is cleared. If the number continues to rise or drop, no additional alarm or alarm history is added. A single baseline and threshold pair—10000 and 10%—is configured and used per IPv4 IP-VPN route target. If the number of routes is not the same as the predefined baseline, the alarm policy for that route target is in effect only after the number exceeds or drops below the baseline.

Table 16-1 CPAM threshold reaching alarms (continued)

Long name/Threshold configuration form name class.AlarmName	Index number	Description
ISIS LSP Alarm Threshold topology.IsisLspThresholdExceeded	375	Raised when the number of LSPs per ISIS routing level in the LSDB of a CPAA reaches or exceeds a predefined value. The number of LSPs is too high.
ISIS LSP Rate Alarm Threshold topology.IsisLspRateThresholdExceeded	376	Raised when the number of LSPs received per second and per ISIS routing level on a CPAA reaches or exceeds a predefined rate.
ISIS Reachability Threshold topology.IsisReachabilityThresholdExceeded	377	Raised when the number of reachabilities per ISIS routing level in the LSDB of a CPAA reaches or exceeds a predefined value. The number of prefixes is too high.
OSPF External LSA Alarm Threshold topology.OspfExternalLsaThresholdExceeded	372	Raised when the number of OSPF external LSAs in the LSDB of a CPAA reaches or exceeds a predefined value. The number of external LSAs is too high.
OSPF LSA Rate Per Router Alarm Threshold topology.OspfLsaRateThresholdExceededPerRouter	308	Raised when the number of OSPF LSAs received per second by a CPAA from a router reaches or exceeds a predefined rate.
OSPF LSA Per Router Alarm Threshold topology.OspfLsaThresholdExceededPerRouter	374	Raised when the number of OSPF LSAs from a router in the LSDB of a CPAA reaches or exceeds a predefined value. The number of LSAs advertised from the router is too high.
OSPF Internal LSA Alarm Threshold topology.OspfInternalLsaThresholdExceededPerArea	309	Raised when the number of internal OSPF LSAs in the LSDB of a CPAA for the specified area reaches or exceeds a predefined value. The number of LSAs advertised in the OSPF area is too high.
OSPF Internal LSA Rate Alarm Threshold topology. OspfInternalLsaRateThresholdExceededPerArea	310	Raised when the number of internal OSPF LSAs received per second for the specific area on a CPAA reaches or exceeds a predefined rate.

The following figure shows an ISIS LSP rate alarm threshold configuration form:

Figure 16-1 ISIS LSP Rate Alarm Threshold configuration form



16.2 Workflow for threshold reaching alarms

16.2.1 Stages

1

Configure alarm thresholds. See 16.3 “To configure alarm thresholds” (p. 295) for more information.

2

View and configure alarm types. See 16.4 “To view and configure alarm types” (p. 297) for more information.

16.3 To configure alarm thresholds

16.3.1 Steps

1

Choose Tools→Route Analysis→Alarm Configuration from the NFM-P main menu. The Alarm Configuration form opens.

2

Ensure that Routing Alarm Type (CPAM: Topology) is selected from the object drop-down menu and click on the Search button. A list of alarms appears.

3

Choose an alarm and click on the Properties button. The Routing Alarm Type - topology.*alarm* (Edit) form opens with the General tab displayed.

4

Click on the Alarm Thresholds tab.

5

Click on the Create button. The *Alarm_long_name* Threshold [Create] form opens, for the selected alarm .

6

Click on the Select button next to the IP Address parameter. The Select CPAA - *Routing_alarm_type* Threshold form opens.

7

Select a CPAA and click on the OK button. The Select CPAA - *Routing_alarm_type* Threshold form closes and the *Routing_alarm_type* Threshold (Create) refreshes with the CPAA information.

8

Configure the Administrative State parameter.

9

Configure the parameter in Table 16-2, “Routing alarm threshold parameters” (p. 296) , depending on the type of routing alarm for which you are configuring the threshold.

Table 16-2 Routing alarm threshold parameters

Routing alarm type	Threshold parameters	Notes
ISIS LSP Rate Alarm Threshold	Level Per (sec) CPAA Instance ID	—
ISIS LSP Alarm Threshold	Level CPAA Instance ID	—
ISIS Reachability Threshold	Level CPAA Instance ID	—
OSPF Internal LSA Alarm Threshold	Area ID	—
OSPF Internal LSA Rate Alarm Threshold	Area ID Per (sec)	—
OSPF External LSA Alarm Threshold	—	—
OSPF LSA Rate Alarm Threshold	Router ID Per (sec)	—
OSPF LSA Alarm Threshold	Area ID Router ID	—
BGP Route High Watermark Per RT Threshold	Type Route Target	—
BGP Route Low Watermark Per RT Threshold	Type Route Target	—
BGP Route Rate Threshold Per RT Threshold	Type Route Target	—
BGP Monitor Prefix Flap Rate Threshold	Per (sec)	—
BGP AS Path Length Per Monitored Prefix Threshold	BGP Prefix Type AS Path Length	You can override or suppress the alarms on the individual BGP monitored prefix. See Chapter 10, “BGP management” for information.
BGP Redundancy Loss Per Monitored Prefix Threshold	BGP Prefix Type Minimum Number of NHops	You can override or suppress the alarms on the individual BGP monitored prefix. See Chapter 10, “BGP management” for information.
BGP Packet Rate Threshold	Type Route Target	—
BGP Route Change Per Next Hop Threshold	BGP Next Hop Change Threshold In Percent (%) Alarm Baseline Reset Interval (hours)	—

Table 16-2 Routing alarm threshold parameters (continued)

Routing alarm type	Threshold parameters	Notes
BGP Route Change Per RT Threshold	Type Route Target Change Threshold In Percent (%) Alarm Baseline Reset Interval (hours)	—
BGP Route Count Threshold	Type	—
BGP Route Flap Rate Threshold	Per (sec)	—
BGP Route Rate Threshold	Per (sec)	—

10

Configure the Routing Alarm Type Threshold parameter, if applicable.

11

Click on the OK button to save the configuration and close the form.

12

Click on the OK button to close the Routing Alarm Type - topology.*alarm* (Edit) form.

13

Close the Alarm Configuration form.

END OF STEPS

16.4 To view and configure alarm types

16.4.1 Steps

1

Choose Tools→Route Analysis→Alarm Configuration from the NFM-P main menu. The Alarm Configuration form opens.

2

In the Object Type drop-down, expand Routing Alarm Threshold (CPAM: Topology), then expand CPAA Alarm Threshold (CPAM: Topology).

3

Choose a type of routing alarm:

- BGP AS Path Length Per Monitored Prefix Threshold (CPAM: Topology)

- BGP Monitor Prefix Flap Rate Threshold (CPAM: Topology)
- BGP Packet Rate Threshold (CPAM: Topology)
- BGP Redundancy Loss Per Monitored Prefix Threshold (CPAM: Topology)
- BGP Monitored Prefix Unreachable Alarm (CPAM: Topology)
- BGP Route Change Per Next Hop Threshold (CPAM: Topology)
- BGP Route Change Per RT Threshold (CPAM: Topology)
- BGP Route Count Threshold (CPAM: Topology)
- BGP Route Flap Rate Threshold (CPAM: Topology)
- BGP Route High Watermark Per RT Threshold (CPAM: Topology)
- BGP Route Low Watermark Per RT Threshold (CPAM: Topology)
- BGP Route Rate Threshold (CPAM: Topology)
- BGP Route Rate Threshold Per RT Threshold (CPAM: Topology)
- ISIS LSP Alarm Threshold (CPAM: Topology)
- ISIS LSP Rate Alarm Threshold (CPAM: Topology)
- ISIS Reachability Threshold (CPAM: Topology)
- OSPF External LSA Alarm Threshold (CPAM: Topology)
- OSPF Internal LSA Alarm Threshold (CPAM: Topology)
- OSPF Internal LSA Rate Alarm Threshold (CPAM: Topology)
- OSPF LSA Per Router Alarm Threshold (CPAM: Topology)
- OSPF LSA Rate Per Router Alarm Threshold (CPAM: Topology)

4

Specify a filter to create a filtered list of alarms, and click on the Search button. A list of alarms appears.

5

Choose an alarm and click on the Properties button. The Routing Alarm Type - topology.*alarm* (Edit) form opens with the General tab displayed.

6

Click on the Alarm Thresholds tab to view configured alarm thresholds.

7

Close the form.

8

Close the Alarm Configuration form.

END OF STEPS

Part VI: Multicast management

Overview

Purpose

This volume provides multicast management information.

Contents

17 Multicast manager

17.1 Multicast manager overview

17.1.1 Introduction

The CPAM multicast manager provides a centralized location for managing multicast domains. You can use the multicast manager to monitor, diagnose, and navigate to multicast objects in service provider multicast networks. The multicast manager allows you to quickly navigate to specific multicast objects—such as, PIM routing instances, groups, or interfaces.

The multicast manager provides a real-time view multicast objects in the network, such as:

- group, source, and multicast tree for a specific (*, G) and (S,G) state
- PIM and IGMP routers
- PIM and IGMP interfaces
- RPs
- candidate RPs
- elected BSRs
- candidate BSRs

The multicast topology view of the network is synchronized with the IGP domain. If you move an object on the IGP topology map, the same object moves on the multicast topology view.

Figure 17-2, “Sample multicast topology view with highlighting” (p. 303) shows a sample multicast topology view.

17.1.2 Multicast networks

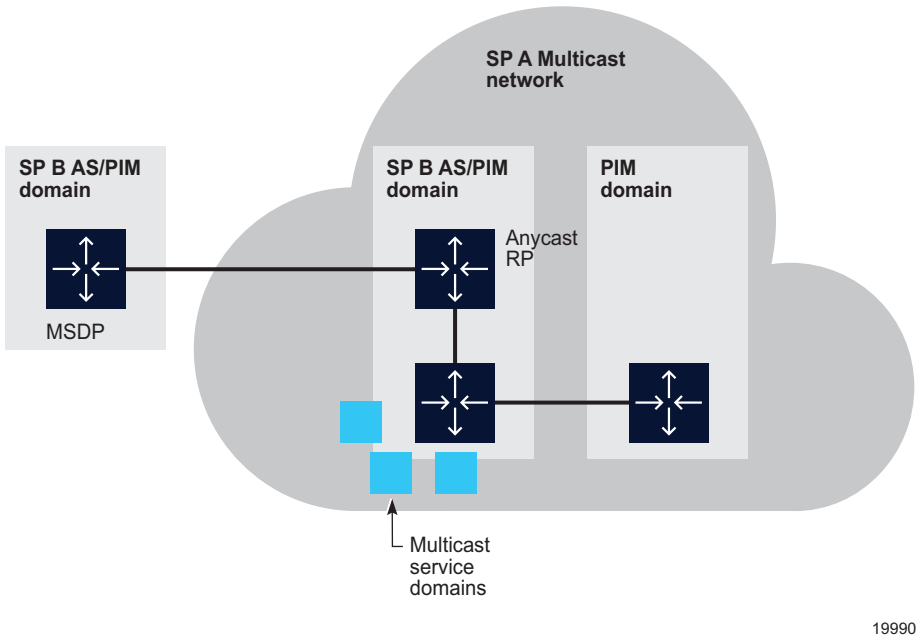
A service provider multicast network typically includes a PIM domain which runs PIM/IGMP snooping, in addition to multiple services—such as an L2 domain.

A PIM domain is a contiguous set of routers that implement PIM and are configured to operate within a common boundary. One router in this domain is elected the BSR and all of the boot strap messages are flooded, hop by hop, until all of the PIM routers learn the same set of RPs.

Multicast services, such as VPLS, implement PIM or IGMP snooping.

The following figure shows a sample multicast network:

Figure 17-1 Sample multicast network



The CPAM supports the following multicast protocols and practices:

- PIM-SM, including SSM, for forwarding state configuration
- manual RP configuration and dynamic BSR, for configuring and distributing PIM RP data
- anycast RP for redundancy

17.2 Monitoring the multicast network

17.2.1 General information

The CPAM generates a multicast topology view for each IGP topology view. IGP routers and IGP links are displayed in grey on the topology view. The coordinates of the routers on the multicast topology view are the same as their coordinates on the IGP and MPLS topology views. If you change the coordinates of a router in one view, the coordinates immediately change in the other two views.

If PIM or IGMP is administratively up and operational on the core routing instance, the router icon changes. The color of the router icon indicates the PIM domain that the router belongs to. The PIM or IGMP interfaces which are administratively and operationally up are displayed in dark green. Otherwise, the interfaces are red.

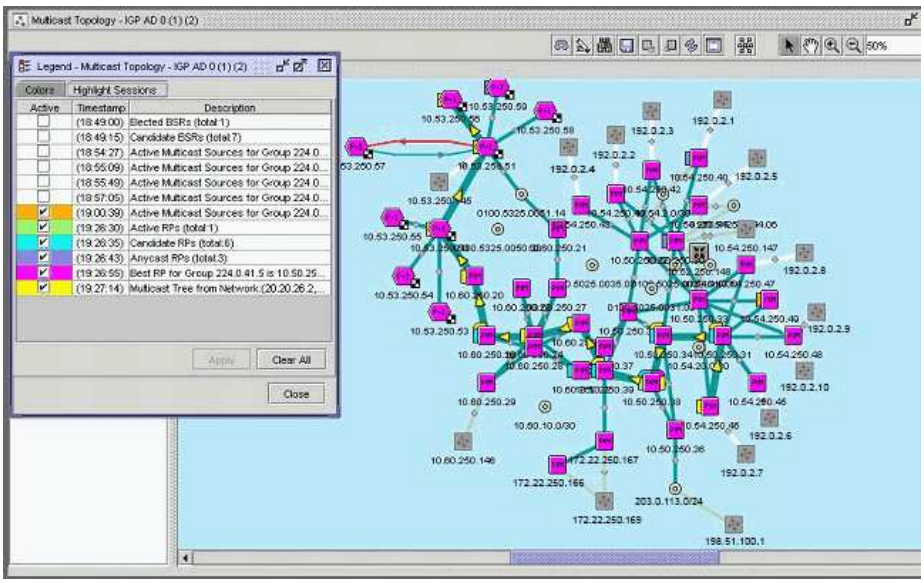
BSR, RP, C-RP, Anycast-RP and MSDP routers do not have an identifying icon. You can highlight these routers. See 17.2.7 “RP, candidate RP, best RP, and anycast RP highlighting” (p. 306) for information.

The icons displayed on the multicast topology view represent the following:

- **PIM-enabled routers**
  These multicast routers are enabled with only PIM.
- **IGMP routers with no IGMP interfaces**
  These multicast routers are enabled with only IGMP and are not configured with IGMP interfaces.
- **IGMP routers with IGMP interfaces**
  These multicast routers are enabled with only IGMP and have at least one IGMP interface.
- **PIM and IGMP routers with no IGMP interfaces**
  These multicast routers are both PIM- and IGMP-enabled and have no IGMP interfaces configured.
- **PIM and IGMP routers with no IGMP interfaces**
  These multicast routers are both PIM- and IGMP-enabled with at least one IGMP interface.

The following figure shows a sample multicast topology view with several highlights.:

Figure 17-2 Sample multicast topology view with highlighting



The CPAM multicast manager displays IGP links with the following colours for PIM links:

- Yellow — PIM link up and IGP link down
- Green — PIM link up and IGP link up
- Red — PIM link down
- Light green — IGP link

17.2.2 Rendezvous point

When a BSR is used, you can retrieve a list of RPs in the network from a router in that domain. When the static RP technique is used, assuming that all of the routers have a consistent configuration, you can retrieve the list of RPs from any router. You can retrieve the CPAM multicast manager RP list for a PIM domain only from the elected BSR.

You can statically define an RP and configure the elected BSR or MSDP. The RP can represent different groups for different configurations. The CPAM creates a global RP object that has different tabs which list different groups for each configuration. An RP in an anycast configuration is the virtual RP and the following information is listed for the RP:

- anycast peers
- peers in other domains (for MSDP RP)
- candidate RPs (BSR)

You can identify an RP on the multicast topology view.

17.2.3 Bootstrap router

All BSRs—including candidate BSRs and elected BSR— are available in the PIM Domain. The CPAM creates a global BSR object.

You can identify the candidate BSR and elected BSR routers in the multicast topology highlight.

17.2.4 Multicast states

The CPAM multicast manager can access all of the multicast states in the NFM-P. The CPAM creates a global multicast state object and populates the object when PIM and IGMP (*,G) and (S,G) state objects are created, modified, or deleted. The CPAM uses the global multicast state object to determine the following:

- the number of (*,G) and (S,G) states that are currently present in the entire network
- the list of all of the PIM and IGMP routers which have multicast states for a (*,G) or (S,G).
- the number of PIM or IGMP routers that have multicast states for a (*,G) or (S,G)
- all of the multicast states in the network without going to all of the multicast routers in the network

The following figure shows the PIM domain form with the States tab displayed.

Figure 17-3 PIM Domain—Multicast states

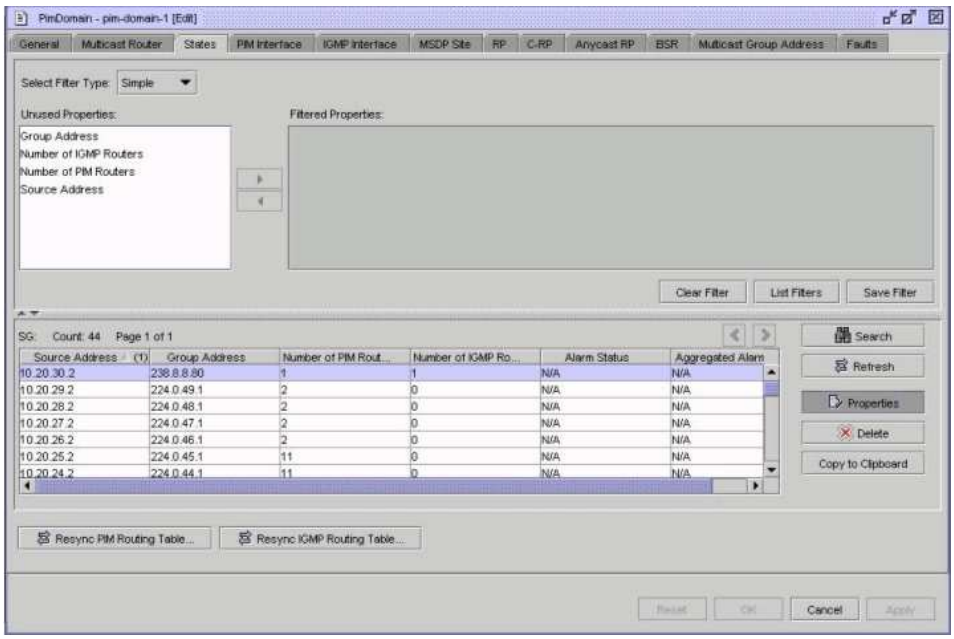
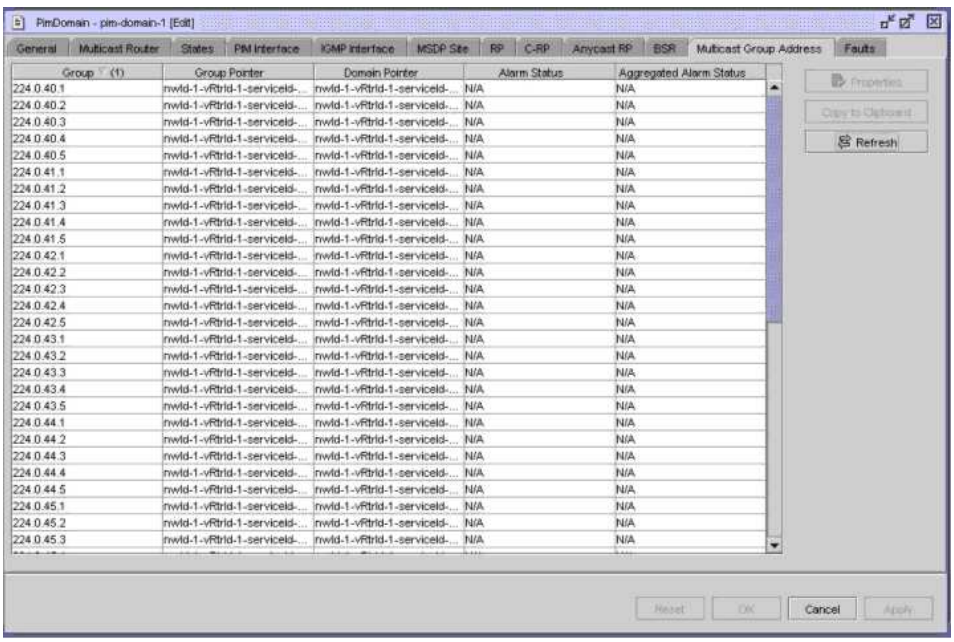


Figure 17-4, “PIM Domain—Multicast Group Address” (p. 305) shows the PIM domain form with the Multicast Group Address tab displayed.

Figure 17-4 PIM Domain—Multicast Group Address



17.2.5 Active multicast sources

You can use the CPAM multicast manager to highlight the active multicast sources for all of the multicast groups, or for a multicast group, on the multicast topology view.

17.2.6 Multicast tree highlighting

You can use the CPAM multicast manager to highlight the multicast tree on the corresponding multicast topology view for a multicast source and group (S,G) or (*,G) pairs. The highlight can be invoked from multicast topology view where the source S=0.0.0.0 for (*,G). The multicast tree can be within one PIM domain or across multiple PIM domains.

When you perform a multicast tree highlight, the CPAM finds all of the PIM routers and determines all of the outgoing interfaces for that specific (S,G) or (*,G) state. The CPAM then asynchronously highlights the multicast tree—PIM routers and PIM interfaces—on the multicast topology view as it receives responses from the routers.

17.2.7 RP, candidate RP, best RP, and anycast RP highlighting

You can use the CPAM to highlight all of the RPs, the best RP for a group, candidate RPs, and anycast RPs on the multicast topology view. In addition, you can highlight the PIM routers that have a different RP table than the elected BSR. To highlight all of the RPs, the CPAM uses the RP table of the BSR router.

17.2.8 Elected BSR and candidate BSR highlighting

You can use the CPAM to highlight all of the elected and candidate RPs. For candidate RPs, the CPAM uses the CPAM BSR objects. To highlight the elected BSR or BSRs, the CPAM uses both the CPAM BSR objects and existing PIM information from the NFM-P. In addition, you can highlight the PIM routers that have different elected BSRs.

17.2.9 OAM multicast tree highlighting

The multicast trace OAM tool, or mtrace, identifies the hop-by-hop route used by VPRN multicast traffic to reach the target router. This multicast trace OAM diagnostic gathers the hop address, routing error conditions, and packet statistics at each hop. The multicast manager attempts to trace the receiver-to-sender route for the traffic. The destination of the diagnostic can be any PIM-enabled interface in the routing instance. The results of the trace are displayed on the multicast topology view.

You can use the multicast trace OAM to build part of a multicast tree for a (S,G) state from a set of DDRs.

17.2.10 Multicast highlighted path audit

You can use the CPAM to perform a path audit on a highlighted multicast tree or OAM multicast tree. After a path resource audit has been performed, you should examine the ingress queues and Auditing MC-Fabric portions of the Audit Results form to ensure that the multicast network is in good health. The audit fails if these portions have failed or if Ingress Switch Fabric Multicast Path is Secondary or Blackhole.

See 7.1 “Map highlighting overview” (p. 85) for information about highlighted path audits. See 17.25 “To perform a highlighted multicast path audit” (p. 333) for information about how to configure the multicast highlighted path audit.

17.2.11 Multicast global info tables

You can use the Global Info Tables option on the multicast topology map to view an info table that displays information about PIM interface attributes on the map. When you configure Global Info Tables to display PIM interface statistics information—such as Number of (S,G) States, Number of (*,G) States, Number of (*, *, RP) States, Tx Packets, or Last States Counter Update—you must first ensure that the statistics collection is manually performed on the PIM interface. You can perform an on-demand statistics collection, or a periodic collection by configuring a MIB entry policy.

See 7.35 “To use the Global Info Tables button” (p. 125) for information about how to configure Global info tables. See 7.37 “To apply an info table configuration to a map highlight” (p. 126) for information about how to apply an info table to a highlight on the multicast topology map.

17.3 Workflow for multicast manager

17.3.1 Stages

1

Ensure that PIM and IGMP are properly configured using the NFM-P.

2

Create a PIM domain. If one PIM domain is used, all of the existing or potential multicast routers could belong to this PIM domain. See 17.4 “To create a PIM domain” (p. 309) for more information.

3

Add PIM and IGMP routers to the PIM domain. See 17.4 “To create a PIM domain” (p. 309) for more information.

4

Create a multicast group. See 17.5 “To create a multicast group” (p. 310) for more information.

5

Populate multicast groups for the multicast network with (*,G) and (S,G) pairs. See 17.6 “To automatically populate a multicast group” (p. 312) for more information.

6

Resynchronize all of the multicast network objects in the CPAM with the NFM-P, as required. See 17.7 “To resync the multicast network” (p. 312) for more information.

7

After a router is added to the PIM domain, you can:

- View PIM interface information. See 17.9 “To view a PIM interface” (p. 314) for more information.
- View IGMP link assocations with PIM interfaces. See 17.10 “To view the IGP link associated with a PIM interface” (p. 315) for more information.
- View IGMP interface information. See 17.11 “To view an IGMP interface” (p. 316) for more information.
- View MSDP information. See 17.12 “To view an MSDP site” (p. 317) for more information.
- View RP information. See 17.13 “To view RP information” (p. 318) for more information.
- View C-RP information. See 17.14 “To view candidate RP information” (p. 320) for more information.
- View anycast RP information. See 17.15 “To view anycast RP information” (p. 321) for more information.
- View BSR information. See 17.16 “To view BSR information” (p. 322) for more information.
- View multicast state information. See 17.17 “To view multicast group information for a PIM domain” (p. 323) for more information.

8

Open the multicast topology view. See 17.8 “To open the multicast topology view” (p. 313) for more information.

9

Highlight RPs on the multicast topology view, as required. See 17.18 “To highlight RPs” (p. 324) for more information.

10

Highlight routers with mismatched RP tables on the multicast topology view, as required. See 17.19 “To highlight routers with mismatched RP tables” (p. 325) for more information.

11

Highlight BSRs on the multicast topology view, as required. See 17.20 “To highlight BSRs” (p. 326) for more information.

12

Highlight routers with mismatched BSRs on the multicast topology view, as required. See 17.21 “To highlight routers with mismatched elected BSRs” (p. 327) for more information.

13

Highlight the multicast tree on the multicast topology view, as required. See 17.22 “To highlight the multicast tree” (p. 329) for more information.

14

Highlight routers for a multicast group or mask on the multicast topology view, as required. See 17.23 “To highlight routers for a multicast group or mask” (p. 331) for more information.

15

Highlight active sources for a group on the multicast topology view, as required. See 17.24 “To highlight active sources for a group” (p. 332) for more information.

16

Perform a highlighted multicast path audit, as required. See 17.25 “To perform a highlighted multicast path audit” (p. 333) for more information.

17

View the legend for a topology map, if required. See 17.26 “To view the legend for a topology map” (p. 335) for more information.

17.4 To create a PIM domain

17.4.1 Steps

1

Choose Tools→Route Analysis→Multicast Manager from the NFM-P main menu. The Multicast Manager form opens.

2

Click on the Create button and choose Pim Domain from the contextual menu. The PimDomain (Create) form opens with the General tab displayed.

3

Configure the parameters:

- Domain id
- Description

4

Click on the Apply button.

5

Click on the Multicast Router tab button.

6

Click on the Add button. The topology.Router search form opens.

7

Specify a filter for the search, if required, and click on the Search button.

8

Choose a router and click on the OK button. The topology.Router search form closes and the PimDomain (Edit) form reappears.

9

Click on the following tab buttons to view PIM and IGMP configuration information:

- States—view multicast states details.
- PIM Interface—view PIM interface details. See 17.9 “To view a PIM interface” (p. 314) .
- IGMP Interface—view IGMP interface details. See 17.11 “To view an IGMP interface” (p. 316) .
- MSDP Site—view MSDP site details. See 17.12 “To view an MSDP site” (p. 317) .
- RP—view RP details. See 17.13 “To view RP information” (p. 318) .
- C-RP—view C-RP details. See 17.14 “To view candidate RP information” (p. 320) .
- Anycast RP—view anycast RP details. See 17.15 “To view anycast RP information” (p. 321) .
- BSR—view BSR details. See 17.16 “To view BSR information” (p. 322) .
- Multicast Groups—view multicast group details. See 17.17 “To view multicast group information for a PIM domain” (p. 323) .
- Faults—view fault information

10

Click on the OK button to close the PimDomain (Edit) form.

11

Close the Multicast Manager form.

END OF STEPS

17.5 To create a multicast group

17.5.1 Steps

1

Choose Tools→Route Analysis→Multicast Manager from the NFM-P main menu. The Multicast Manager form opens.

2

Click on the Create button and choose Group from the contextual menu. The Multicast Group Address (Create) form opens with the General tab displayed.

3

Configure the Group Address parameter.

4

Click on the Sources tab button.

5

Click on the Create button. The Multicast Source Address (Create) form opens.

6

Configure the Multicast Source Address parameter.

7

Click on the OK button. The Multicast Source Address (Create) form closes.

8

Repeat Step 5 to Step 7 to add additional multicast source addresses, if required.

9

Click on the Domains tab button.

10

Click on the Create button. The Group Domain Binding (Create) form opens.

11

Click on the Select button next to the Domain id parameter. The Select Domain Pointer - Group Domain Binding form opens.

12

Choose an entry and click on the OK button. The Select Domain Pointer - Group Domain Binding form closes.

13

Click on the OK button. The Group Domain Binding (Create) form closes.

14

Repeat Step 10 to Step 13 , if required.

15

Click on the OK button. The Multicast Group Address (Create) form closes.

16

Close the Multicast Manager.

END OF STEPS

17.6 To automatically populate a multicast group

17.6.1 Steps

1

Choose Tools→Route Analysis→Multicast Manager from the NFM-P main menu. The Multicast Manager form opens.

2

Click on the Populate button and choose Auto Populate Multicast Groups.

3

Close the Multicast Manager.

END OF STEPS

17.7 To resync the multicast network

17.7.1 When to use

Perform the following procedure to resynchronize all of the multicast network objects in the CPAM with the NFM-P. Nokia recommends that you resync the entire multicast network before you perform any operation on the multicast map.

17.7.2 Steps

1

Choose Tools→Route Analysis→Multicast Manager from the NFM-P main menu. The Multicast Manager form opens.

2

Click on the Search button. A list of multicast domains appears.

3

Choose a domain and click on the Properties button. The PimDomain (Edit) form opens with the General tab displayed.

4

Click on the Resync All from Network button. A dialog box appears.

5

WARNING

Equipment Damage

Resynchronizing the network may take several minutes, depending on the size of the network.

Click on the Yes button to resynchronize all of the routers in the PIM domain with the NFM-P.

END OF STEPS

17.8 To open the multicast topology view

17.8.1 Steps

1

Choose Tools→Route Analysis→Multicast Manager from the NFM-P main menu. The Multicast Manager form opens.

2

Click on the Multicast Topology button. The multicast topology view may take several minutes to load.

Note: The multicast topology view is synchronized in real-time with the IGP topology maps. If you move an object on an IGP topology view, the same object moves on the multicast topology view. If you move an object on the multicast topology view, the same object moves on the IGP topology view.

3

Perform one of the following:

a. Highlight RPs—active RPs, candidate RPs, best RP for a group, or anycast RPs. See 17.18 “To highlight RPs” (p. 324) .

b. Highlight BSRs—elected BSRs or candidate BSRs. See 17.20 “To highlight BSRs” (p. 326) .

c. Highlight the multicast tree—multicast tree from the network, historical multicast tree, or OAM multicast tree. See 17.22 “To highlight the multicast tree” (p. 329) .

d. Highlight active sources for a group. See 17.24 “To highlight active sources for a group” (p. 332) .

4

Close the multicast topology view.

5

Close the Multicast Manager form.

END OF STEPS

17.9 To view a PIM interface

17.9.1 Steps

1

Choose Tools→Route Analysis→Multicast Manager from the NFM-P main menu. The Multicast Manager form opens.

2

Specify a filter for the search, if required, and click on the Search button. A list of domains appears.

3

Choose an entry and click on the Properties button. The PimDomain (Edit) form opens with the General tab displayed.

4

Click on the PIM Interface tab button.

5

Specify a filter for the search, if required, and click on the Search button. A list of PIM interfaces appears.

6

Choose an entry and click on the Properties button. The PIM Interface (Edit) form opens with the General tab displayed.

7

Click on the following tab buttons to view and configure the PIM interface:

- Behavior
- Multicast CAC
- Neighbor
- Statistics
- Faults

Note: See the “PIM configuration procedures” section in the *NSP NFM-P Classic Management User Guide* for information about how to configure PIM interfaces.

8

Close the PIM Interface (Edit) form.

9

Close the PimDomain (Edit) form.

10

Close the Multicast Manager form.

END OF STEPS

17.10 To view the IGP link associated with a PIM interface

17.10.1 Steps

1

Choose Tools→Route Analysis→Multicast Manager from the NFM-P main menu. The Multicast Manager form opens.

2

Specify a filter for the search, if required, and click on the Search button. A list of domains appears.

3

Choose an entry and click on the Properties button. The PimDomain (Edit) form opens with the General tab displayed.

4

Click on the PIM Interface tab button.

5

Specify a filter for the search, if required, and click on the Search button. A list of PIM interfaces appears.

6

Choose an entry and click on the Properties button. The PIM Interface (Edit) form opens with the General tab displayed.

7

Click on the Properties button next to the Link Data parameter in the IGP Link panel to view the IGP link associated with the PIM interface. The *Type* Link (Edit) form opens with the General tab displayed.

8

Click on the tab buttons to view information about the link.

9

Close the *Type* Link (Edit) form.

10

Close the PimDomain (Edit) form.

END OF STEPS

17.11 To view an IGMP interface

17.11.1 Steps

1

Choose Tools→Route Analysis→Multicast Manager from the NFM-P main menu. The Multicast Manager form opens.

2

Specify a filter for the search, if required, and click on the Search button. A list of domains appears.

3

Choose an entry and click on the Properties button. The PimDomain (Edit) form opens with the General tab displayed.

4

Click on the IGMP Interface tab button.

5

Specify a filter for the search, if required, and click on the Search button. A list of IGMP interfaces appears.

6

Choose an entry and click on the Properties button. The IGMP Interface (Edit) form opens with the General tab displayed.

7

Click on the following tab buttons to view and configure the IGMP interface:

- Behavior
- Multicast CAC
- Multicast Group
- Multicast Group/Source
- Static Group/Source
- Statistics
- Faults

Note: See “IGMP configuration workflow and procedures” in the *NSP NFM-P Classic Management User Guide* for information about how to configure IGMP interfaces.

8

Close the IGMP Interface (Edit) form.

9

Close the PimDomain (Edit) form.

10

Close the Multicast Manager form.

END OF STEPS

17.12 To view an MSDP site

17.12.1 Steps

1

Choose Tools→Route Analysis→Multicast Manager from the NFM-P main menu. The Multicast Manager form opens.

2

Specify a filter for the search, if required, and click on the Search button. A list of domains appears.

3

Choose an entry and click on the Properties button. The PimDomain (Edit) form opens with the General tab displayed.

4

Click on the MSDP Site tab button. A list of MSDP sites appears.

5

Choose an entry and click on the Properties button. The MSDP (Edit) form opens with the General tab displayed.

6

Click on the following tab buttons to view and configure the MSDP site:

- Group
- Peer
- Source
- Import Policies
- Export Policies
- Data Source Active
- Statistics
- Faults

Note: See “MSDP configuration workflow and procedures” in the *NSP NFM-P Classic Management User Guide* for information about how to configure MSDP sites.

7

Close the MSDP (Edit) form.

8

Close the PimDomain (Edit) form.

9

Close the Multicast Manager form.

END OF STEPS

17.13 To view RP information

17.13.1 Steps

1

Choose Tools→Route Analysis→Multicast Manager from the NFM-P main menu. The Multicast Manager form opens.

2

Specify a filter for the search, if required, and click on the Search button. A list of domains appears.

3

Choose an entry and click on the Properties button. The PimDomain (Edit) form opens with the General tab displayed.

4

Click on the RP tab button. A list of rendez-vous points is displayed.

5

Choose an entry and click on the Properties button. The RP (Edit) form opens with the General tab displayed.

6

Click on the Group Prefix in RP Table tab button to view a list of group prefixes in the RP table.

7

Choose an entry and click on the Properties button. The Group Prefix in RP Table (Edit) form opens.

8

View the following group prefix properties:

- group prefix
- group mask
- RP set type
- C-RP hold time
- C-RP expiry time
- C-RP priority

Note: See “To configure PIM on a routing instance” in the *NSP NFM-P Classic Management User Guide* for information about how to configure an RP.

9

Close the Group Prefix in RP Table (Edit) form.

10

Close the RP (Edit) form.

11

Close the PimDomain (Edit) form.

12

Close the Multicast Manager form.

END OF STEPS

17.14 To view candidate RP information

17.14.1 Steps

1

Choose Tools→Route Analysis→Multicast Manager from the NFM-P main menu. The Multicast Manager form opens.

2

Specify a filter for the search, if required, and click on the Search button. A list of domains appears.

3

Choose an entry and click on the Properties button. The PimDomain (Edit) form opens with the General tab displayed.

4

Click on the C-RP tab button. A list of candidate rendez-vous points is displayed.

5

Choose an entry and click on the Properties button. The C-RP Group Prefix (Edit) form opens with the General tab displayed.

6

Click on the Faults tab button to view fault information.

Note: See “To configure PIM on a routing instance” in the *NSP NFM-P Classic Management User Guide* for information about how to configure a candidate RP.

7

Close the C-RP Group Prefix (Edit) form.

8

Close the PimDomain (Edit) form.

9

Close the Multicast Manager form.

END OF STEPS

17.15 To view anycast RP information

17.15.1 Steps

1

Choose Tools→Route Analysis→Multicast Manager from the NFM-P main menu. The Multicast Manager form opens.

2

Specify a filter for the search, if required, and click on the Search button. A list of domains appears.

3

Choose an entry and click on the Properties button. The PimDomain (Edit) form opens with the General tab displayed.

4

Click on the Anycast RP tab button. A list of anycast rendez-vous points is displayed.

5

Choose an entry and click on the Properties button. The Anycast RP (Edit) form opens with the General tab displayed.

6

Click on the following tab buttons to view and configure the anycast RP:

- Anycast Peer
- Faults

Note: See “To configure PIM on a routing instance” in the *NSP NFM-P Classic Management User Guide* for information about how to configure an anycast RP.

7

Close the Anycast RP (Edit) form.

8

Close the PimDomain (Edit) form.

9

Close the Multicast Manager form.

END OF STEPS

17.16 To view BSR information

17.16.1 Steps

1

Choose Tools→Route Analysis→Multicast Manager from the NFM-P main menu. The Multicast Manager form opens.

2

Specify a filter for the search, if required, and click on the Search button. A list of domains appears.

3

Choose an entry and click on the Properties button. The PimDomain (Edit) form opens with the General tab displayed.

4

Click on the BSR tab button. A list of BSRs is displayed.

5

Choose an entry and click on the Properties button. The BSR (Edit) form opens with the BootStrap Router tab displayed.

6

View the BSR properties.

7

Click on the Faults tab button to view faults information.

Note: See “To configure PIM on a routing instance” in the *NSP NFM-P Classic Management User Guide* for information about how to configure a BSR.

8

Close the BSR (Edit) form.

9

Close the PimDomain (Edit) form.

10

Close the Multicast Manager form.

END OF STEPS

17.17 To view multicast group information for a PIM domain

17.17.1 Steps

1

Choose Tools→Route Analysis→Multicast Manager from the NFM-P main menu. The Multicast Manager form opens.

2

Specify a filter for the search, if required, and click on the Search button. A list of domains appears.

3

Choose an entry and click on the Properties button. The PimDomain (Edit) form opens with the General tab displayed.

4

Click on the Multicast Group tab button. A list of multicast groups is displayed.

5

Choose an entry and click on the Properties button. The Group Domain Binding (Edit) form opens with the General tab displayed.

6

View the multicast group properties.

7

Click on the Faults tab button to view faults information.

Note: See “To configure PIM on a routing instance” in the *NSP NFM-P Classic Management User Guide* for information about how to configure a multicast group.

8

Close the Group Domain Binding (Edit) form.

9

Close the PimDomain (Edit) form.

10

Close the Multicast Manager form.

END OF STEPS

17.18 To highlight RPs

17.18.1 Steps

1

Perform 17.8 “To open the multicast topology view” (p. 313) to open the multicast topology view.

2

Right-click on the view and choose Highlight RPs from the contextual menu.

3

Choose one of the following options:

- Active RPs—to highlight active RPs in the multicast network. Go to Step 4 .
- Candidate RPs—to highlight candidate RPs in the multicast network. The Select Candidate RP Filter form opens. Go to Step 5 .
- Best RP for a Given Group—to highlight the best RP for a specific multicast group. The Highlight Best RP for a Given Group form opens with the General tab displayed. Go to Step 6 .
- Anycast RPs—to highlight anycast RPs. The Select Anycast RP Filter form opens. Go to Step 7 .
- Highlight Routers with Mismatch RP Table—to highlight PIM routers that have a different RP table from the elected BSR. The Highlight Routers with Mismatch RP-Table form opens. Go to 17.19 “To highlight routers with mismatched RP tables” (p. 325) .

4

View the highlighted active RPs on the map. Go to Step 8 .

5

Specify a filter for the search and click on the OK button. The candidate RPs appear on the map. Go to Step 8 .

6

Perform the following steps to highlight the best RP for a multicast group.

1. Click on the Select button next to the Multicast Group Address parameter. The Select Multicast Group form opens.
2. Specify a filter for the search, if required, and click on the Search button. A list of multicast groups appears.

3. Choose an entry and click on the OK button. The Highlight Best RP for a Given Group form refreshes with the multicast group IP address.
4. Click on the OK button. The Highlight Best RP for a Given Group form closes and the best RP for the specified multicast group is highlighted on the multicast topology view.
5. Go to Step 8 .

7

Specify a filter for the search, if required, and click on the OK button. The Select Anycast RP Filter form closes and the anycast RPs are highlighted on the multicast topology view.

8

Click on the Legend button at the top of the topology map and choose Highlight Sessions from the contextual menu. The Legend - Multicast Topology form opens with the Highlight Sessions tab displayed. See 7.32 “To manage active highlights on a topology map” (p. 123) for information about how to manage active highlights on a topology map.

9

Close the multicast topology view.

10

Close the Multicast Manager form.

END OF STEPS

17.19 To highlight routers with mismatched RP tables

17.19.1 Steps

1

Perform 17.8 “To open the multicast topology view” (p. 313) to open the multicast topology view.

2

Right-click on the view and choose Highlight RPs→Highlight Routers with Mismatch RP-Table from the contextual menu. The Highlight Routers with Mismatch RP-Table form opens.

3

Click on the Select button next to the PIM Domain parameter. The Select PIM Domain form opens.

4

Specify a filter for the search, if required, and click on the Search button. A list of PIM domains appears.

5

Select the PIM domain and click on the OK button. The Select PIM Domain form closes.

6

Click on the OK button. The Highlight Routers with Mismatch RP-Table form closes and the PIM routers whose RP table does not match the RP table of the elected BSR are highlighted on the map.

7

Click on the Legend button at the top of the topology map and choose Highlight Sessions from the contextual menu. The Legend - Multicast Topology form opens with the Highlight Sessions tab displayed. You can view the RP table in the Description field of the highlight entry.

See 7.32 “To manage active highlights on a topology map” (p. 123) for information about how to manage active highlights on a topology map.

8

Double-click on the highlighted PIM router. The Router (Edit) form opens with the General tab displayed.

9

Click on the Multicast tab button.

10

Click on the Properties button next to the Site ID parameter in the PIM panel. The PIM Site (Edit) form opens with the General tab displayed.

11

Click on the Group to RP tab button and click on the Rendezvous Point Table tab button to view the RP table.

Note: If you open a PIM router that is not highlighted as mismatched, the RP table would differ from the highlighted PIM router.

END OF STEPS

17.20 To highlight BSRs

17.20.1 Steps

1

Perform 17.8 “To open the multicast topology view” (p. 313) to open the multicast topology view.

2

Right-click on the map and choose Highlight BSRs from the contextual menu.

3

Choose one of the following options:

- Elected BSRs—to highlight the elected BSRs in the multicast network. The Select BSR Filter form opens. Go to Step 4 .
- Candidate BSRs—to highlight candidate BSRs in the multicast network. The Select BSR Filter form opens. Go to Step 5 .
- Highlight Routers with Mismatched Elected BSR—to highlight PIM routers that do not have the same elected BSR. See 17.21 “To highlight routers with mismatched elected BSRs” (p. 327) for information.

4

Specify a filter for the search and click on the OK button. The elected BSRs appear on the map. Go to Step 6 .

5

Specify a filter for the search and click on the OK button. The candidate BSRs appear on the map. Go to Step 6 .

6

Click on the Legend button at the top of the topology map and choose Highlight Sessions from the contextual menu. The Legend - Multicast Topology form opens with the Highlight Sessions tab displayed. See 7.32 “To manage active highlights on a topology map” (p. 123) for information about how to manage active highlights on a topology map.

7

Close the multicast topology view.

8

Close the Multicast Manager form.

END OF STEPS

17.21 To highlight routers with mismatched elected BSRs

17.21.1 Steps

1

Perform 17.8 “To open the multicast topology view” (p. 313) to open the multicast topology view.

2

Right-click on the map and choose Highlight BSRs→Highlight Routers with Mismatch Elected-BSR from the contextual menu. The Highlight Routers with Mismatched Elected-BSR form opens.

3

Click on the Select button next to the PIM Domain parameter. The Select PIM Domain form opens.

4

Select a PIM domain and click on the OK button. The Select PIM Domain form closes.

5

Click on the OK button. The Highlight Routers with Mismatch Elected-BSR form closes and the PIM routers view of the elected BSR is not the same as the real elected BSR are highlighted on the map.

6

Click on the Legend button at the top of the topology map and choose Highlight Sessions from the contextual menu. The Legend - Multicast Topology form opens with the Highlight Sessions tab displayed. You can view the eBSR and the number of eBSRs found in the Description field of the highlight entry.

See 7.32 “To manage active highlights on a topology map” (p. 123) for information about how to manage active highlights on a topology map.

7

Double-click on a highlighted PIM router. The Router (Edit) form opens with the General tab displayed.

8

Click on the Multicast tab button.

9

Click on the Properties button next to the Site ID parameter in the PIM panel. The PIM Site (Edit) form opens with the General tab displayed.

10

Click on the Resync button. A dialog box appears.

11

Click on the Yes button.

12

Click on the RP Behaviour tab button. The eBSR information is displayed in the Elected BootStrap Router panel.

END OF STEPS

17.22 To highlight the multicast tree

17.22.1 Steps

1

Perform 17.8 “To open the multicast topology view” (p. 313) to open the multicast topology view.

2

Right-click on the map and choose Highlight Multicast Tree from the contextual menu.

3

Choose one of the following options:

- Multicast Tree From Network—to highlight the multicast tree from the multicast network. The Highlight Multicast Tree form opens. Go to Step 4 .
- Historical Multicast Tree—to view the historical results of the multicast tree in the multicast network. The Find Historical Multicast Tree form opens. Go to Step 5 .
- OAM Multicast Tree—to highlight an OAM multicast tree. The Highlight OAM Multicast Tree form opens. Go to Step 6 .
- Historical OAM Multicast Tree—to view the historical mtrace OAM results in the multicast network. The Historical Multicast Tree form opens. Go to Step 7 .

4

Perform the following steps to highlight the multicast tree.

1. Click on the Select button next to the Group IP parameter. The Select Multicast Group form opens.
2. Specify a filter for the search, if required, and click on the Search button.
3. Choose an entry and click on the OK button. The Select Multicast Group form closes.
4. Click on the Select button next to the Source IP parameter. The Select Multicast Source form opens.
5. Specify a filter for the search, if required, and click on the Search button.
6. Choose an entry and click on the OK button. The Select Multicast Source form closes.
7. Click on the OK button. The Highlight Multicast Tree form closes and the multicast tree is highlighted on the map.
8. Go to Step 8 .

5

Perform the following steps to highlight a historical multicast tree.

1. Specify a filter for the search, if required, and click on the Search button. A list of historical multicast trees appears.
2. Choose an entry and click on the OK button. The Find Historical Multicast Tree form closes and the selected historical multicast tree is highlighted on the map.

3. Go to Step 8 .

6

Perform the following steps to highlight an OAM multicast tree.

1. Click on the Select button next to the Group IP parameter. The Select Multicast Group form opens.
2. Specify a filter for the search, if required, and click on the Search button.
3. Choose an entry and click on the OK button. The Select Multicast Group form closes.
4. Click on the Select button next to the Source IP parameter. The Select Multicast Source form opens.
5. Specify a filter for the search, if required, and click on the Search button.
6. Choose an entry and click on the OK button. The Select Multicast Source form closes.
7. Click on the Select button next to the Test Routers parameter. The Select Multicast Router form opens.
8. Specify a filter for the search, if required, and click on the Search button.
9. Choose an entry and click on the OK button. The Select Multicast Router form closes.
10. Click on the Execute button to start the test.
11. Click on the Result button. The Result form opens.
12. Specify a filter for the search, if required, and click on the Search button. A list of results of the test appears.
13. Choose an entry and click on the OK button. The mtrace Result Test (Edit) form opens with the General tab displayed. Click on the tabs to view information about the results.
14. Close the mtrace Result Test (Edit) form.
15. Close the Result form.
16. Close the Highlight OAM Multicast Tree form.
17. Go to Step 9 .

7

Perform the following steps to view and highlight the historical results of an OAM multicast tree.

1. Specify a filter for the search, if required, and click on the Search button. A list of historical mtrace results appears.
2. Choose an entry and click on the OK button. The Historical OAM Multicast Tree form closes and the selected historical OAM mtrace results are highlighted on the map.
3. Go to Step 8 .

8

Click on the Legend button at the top of the topology map and choose Highlight Sessions from the contextual menu. The Legend - Multicast Topology form opens with the Highlight Sessions tab displayed. See 7.32 “To manage active highlights on a topology map” (p. 123) for information about how to manage active highlights on a topology map.

9

Close the multicast topology view.

10

Close the Multicast Manager form.

END OF STEPS

17.23 To highlight routers for a multicast group or mask

17.23.1 Steps

1

Perform 17.8 “To open the multicast topology view” (p. 313) to open the multicast topology view.

2

Right-click on the map and choose Highlight Routers for a Multicast Group / Mask from the contextual menu. The Highlight Routers for a Multicast Group / Mask form opens.

3

Click on the Select button next to the Multicast Group Prefix parameter. The Select Multicast Group form opens.

4

Specify a filter for the search, if required, and click on the Search button.

5

Choose an entry and click on the OK button. The Select Multicast Group form closes.

6

Configure the parameters:

- Mask
- Protocol

7

Click on the OK button. The Highlight Routers for a Mulitcast Group / Mask form closes and the multicast routers with the selected protocol for the selected multicast group prefix are highlighted on the map.

8

Click on the Legend button at the top of the topology map and choose Highlight Sessions from the contextual menu. The Legend - Multicast Topology form opens with the Highlight Sessions

tab displayed. See 7.32 “To manage active highlights on a topology map” (p. 123) for information about how to manage active highlights on a topology map.

9

Close the multicast topology view.

10

Close the Multicast Manager form.

END OF STEPS

17.24 To highlight active sources for a group

17.24.1 Steps

1

Perform 17.8 “To open the multicast topology view” (p. 313) to open the multicast topology view.

2

Right-click on the map and choose Highlight Active Sources for a Given Group from the contextual menu. The Highlight Active Sources for a Given Group form opens.

3

Click on the Select button next to the Multicast Group Address parameter. The Select Multicast Group form opens.

4

Specify a filter for the search, if required, and click on the Search button.

5

Choose an entry and click on the OK button. The Select Multicast Group form closes.

6

Click on the OK button. The Highlight Active Sources for a Given Group form closes and the active sources for the selected multicast group are highlighted on the map.

7

Click on the Legend button at the top of the topology map and choose Highlight Sessions from the contextual menu. The Legend - Multicast Topology form opens with the Highlight Sessions tab displayed. See 7.32 “To manage active highlights on a topology map” (p. 123) for information about how to manage active highlights on a topology map.

8

Close the multicast topology view.

9

Close the Multicast Manager form.

End of steps

17.25 To perform a highlighted multicast path audit

17.25.1 Steps

1

Choose Tools→Route Analysis→Multicast Manager from the NFM-P main menu. The Multicast Manager form opens.

2

Click on the Multicast Topology button. The multicast topology view may take several minutes to load.

Note: The multicast topology view is synchronized in real-time with the IGP topology maps. If you move an object on an IGP topology view, the same object moves on the multicast topology view. If you move an object on the multicast topology view, the same object moves on the IGP topology view.

3

Highlight either Multicast tree from network or OAM multicast tree. See 17.22 “To highlight the multicast tree” (p. 329) .

4

Click on the Legend button at the top of the topology map and choose Highlight Sessions from the contextual menu. The Legend-*topology* form opens with the Highlight Sessions tab displayed.

5

Select and right-click on the highlight that you want to audit and choose Audit→ Path Resource Audit from the contextual menu. The Execute - Path Resource Audit form opens.

6

Configure the Stats Capture Delay (s) parameter.

7

Configure the Threshold parameter for the following audit parameters, if required:

- Utilization
- Interface Error
- Ethernet Error
- Section - Severely Errored Seconds
- Section - Severely Errored Framing Seconds
- Line - Severely Errored Seconds
- Total Drop
- In Profile Drop
- Out of Profile Drop

8

Click on the Execute button to begin the audit. The Execute - Path Resource Audit form closes and the Legend - Topology form reappears.

Note: The audit may take several minutes. The icons on the topology map indicate the audit status. Click on the Icons tab on the Legend - Topology form to view the icon definitions.
To cancel the audit, select and right-click on the highlight for which you want to cancel the audit and choose Cancel Audit from the contextual menu. Alternatively, choose Application→Task manager. The Task Manager form opens. Choose the audit task and click on the OK button to open the Task form. Click on the Cancel Task button and confirm the cancellation.

9

On the Legend - Topology form, right-click on the audited highlighted path and choose Show Audit Results from the contextual menu. The Audit Results form opens.

Note: Alternatively, right-click on a highlighted link and choose Show Audit Results from the contextual menu. The Audit Results form opens with the results from the audit on the highlighted link that you selected.

10

Close the Audit Results form.

11

Clear the audit results, if necessary, by right-clicking on the audited highlighted path on the Legend - Topology form and choosing Clear Audit Results.

12

Close the Legend - Topology form.

13

Close the topology map.

END OF STEPS

17.26 To view the legend for a topology map

17.26.1 Steps

1

Perform 17.8 “To open the multicast topology view” (p. 313) to open the multicast topology view.

2

Click on the Legend button at the top of the topology map and choose Colors Legend from the contextual menu. The Legend - Multicast Topology - *IGP_Administrative_Domain* form opens with the Colors tab displayed.

3

Close the Legend - Multicast Topology - *IGP_Administrative_Domain* form.

END OF STEPS

Part VII: Impact analysis

Overview

Purpose

This volume provides impact analysis information.

Contents

18 Impact analysis

18.1 Impact analysis overview

18.1.1 Introduction to impact analysis

You can use the CPAM to analyze the impact of a network failure on services, IP paths, and LSPs, in addition to configuration changes, dynamic changes such as LSP configuration, and reroutes, during a specified time period.

18.1.2 IGP history

You can use checkpoints to compare historical topology changes within a specified interval on the IGP topology map. See 18.1.3 “Topology checkpoints” (p. 340) for information about checkpoints.

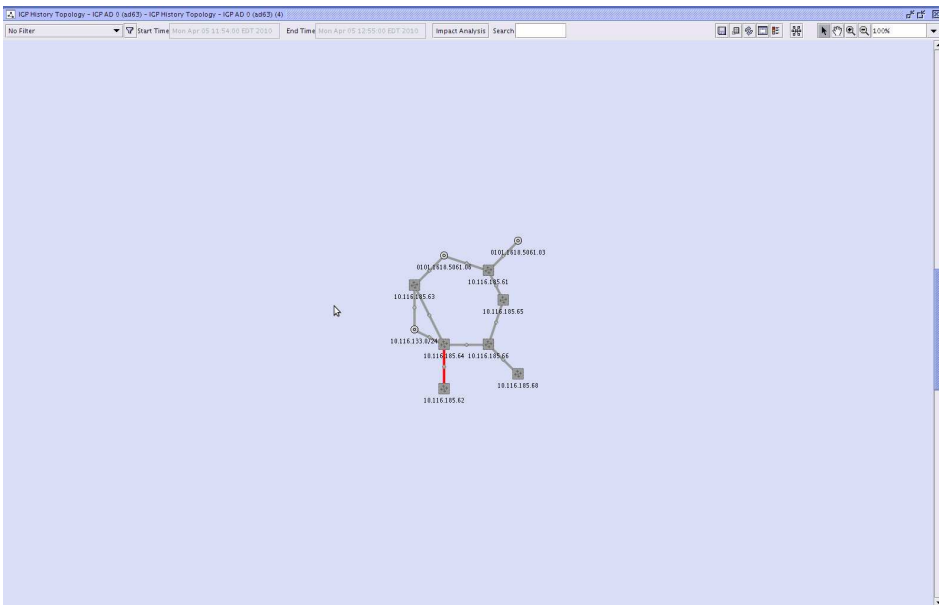
You can compare two checkpoints in the selected interval to view property changes on objects that belong to both checkpoints. The CPAM uses the checkpoints that are closest to the selected interval. See 18.1.4 “Troubleshooting the network by comparing checkpoints” (p. 345) for information.

If checkpoints have been created and not cleaned up during the selected interval, the IGP history window shows topology changes during the interval. Changes are displayed in different colors and line types. The following link colours indicate topology changes between the start and end of the interval:

- grey—no change to operational state or properties
- green—links added
- dashed green line with yellow outline—links added with property changes over interval
- red—links deleted (operational state down at end of interval, missing link)
- dashed red line with yellow outline—property changes during interval and links deleted (operational state down at end of interval, missing link)
- yellow—some properties on the link changed; no changes to operational state
- purple—more than one change to operational state occurred during interval, which may indicate link flapping
- purple dashed line with yellow outline—properties changed during interval and operational state changed at least once during interval (property change and flapping)

The following figure shows an IGP history topology map:

Figure 18-1 IGP history topology map



18.1.3 Topology checkpoints

A checkpointed object is a snapshot of a real topology object at a specific time. When you apply a checkpoint to a real network object, all of the properties of the real object at checkpoint time—for example, metric and bandwidth on IGP links—are copied to the checkpointed object. A checkpointed object is displayed in the same manner as the real topology object, and shares the same OSS class name.

After you have set up the network and the network is operational, you can checkpoint the network to create a snapshot of the current state—which can include routers, links, metric configuration, or bandwidth usage—and compare it with checkpoints collected at different times. In addition, you can compare the results on an IGP history map.

Note: If one or more links go down and are cleaned up between two checkpoints being taken, there will be no indication on the IGP history map that these links were down. From the perspective of a user, the IGP history map shows no changes within their network.

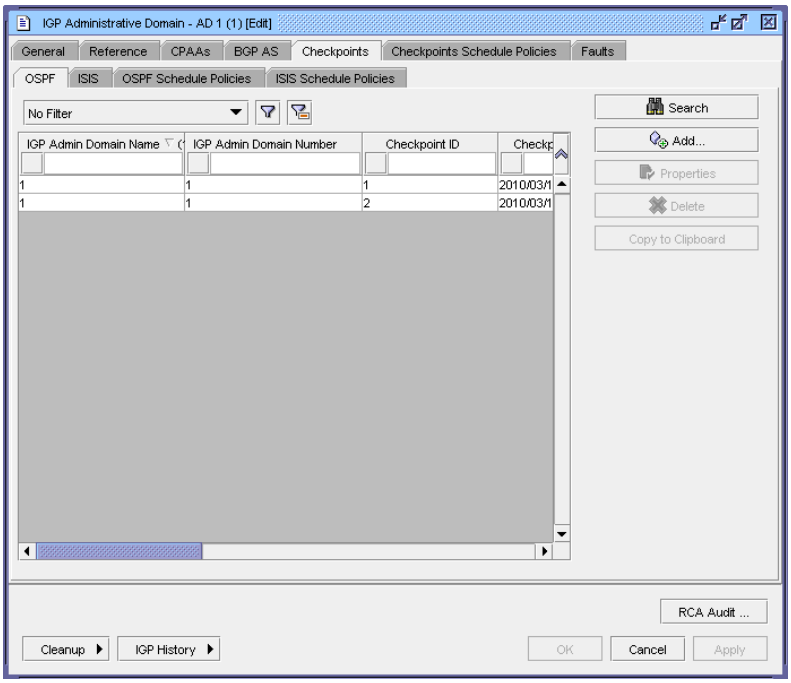
An OSPF topology checkpoint is created for all of the OSPF areas within an IGP administrative domain. See “OSPF checkpoints” (p. 341) for information about OSPF topology checkpoints. An ISIS topology checkpoint is created for all of the ISIS routing domains—Level 2 or Level 1—within an IGP administrative domain. See “ISIS checkpoints” (p. 342) for information about ISIS topology checkpoints.

Note: In OSPF, a routing domain is an OSPF area. In ISIS, a routing domain does not map to the ISIS area, but rather a group of routers that are participating in an ISIS level.

The OSPF and ISIS topology checkpoints are objects of the IGP administrative domain object.

The figure below shows the properties form for an IGP administrative domain. The OSPF and ISIS checkpoints within the IGP administrative domain are listed. In addition, you can access checkpoint schedule policies for the IGP administrative domain.

Figure 18-2 IGP administrative domain



OSPF checkpoints

You can create an OSPF checkpoint for all of the OSPF areas within an IGP administrative domain.

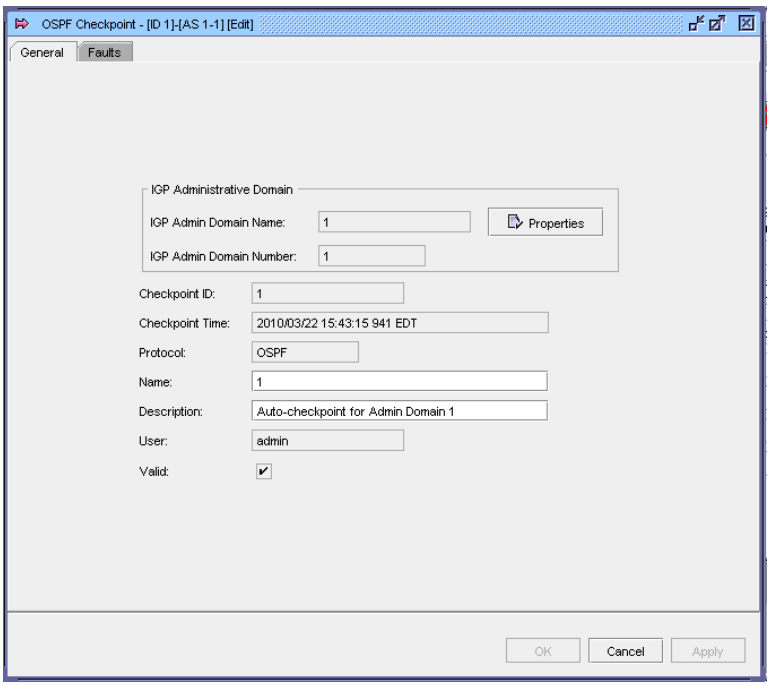
The OSPF objects that are included in an OSPF checkpoint are:

- OSPF area
  - backbone
  - standard
  - stub
  - total stub
  - NSSA no type 5
  - NSSA no summaries
- all of the OSPF area links (point-to-point and broadcast)
- all of the OSPF routers
  - ABR
  - ASBR
  - NFM-P-managed
  - third-party-managed

- OSPF area subnets
- CPAA

The following figure shows the properties form for an OSPF checkpoint:

Figure 18-3 OSPF checkpoint



ISIS checkpoints

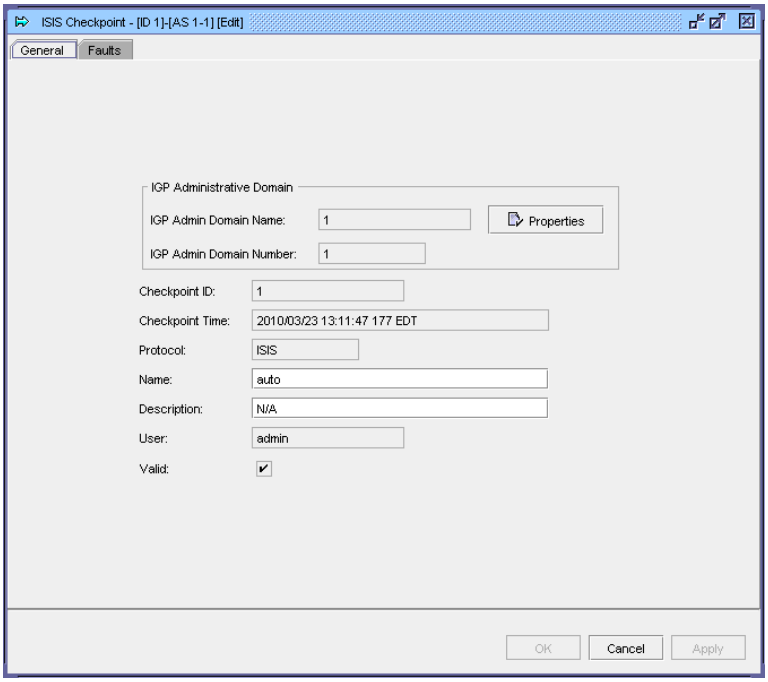
You can create an ISIS checkpoint for all of the ISIS routing domains within an IGP administrative domain.

The ISIS objects that are included in an ISIS checkpoint are:

- all of the ISIS routing domain links (point-to-point and broadcast)
- all of the ISIS routers
  - L1
  - L2
  - L1/L2
  - ASBR
  - NFM-P-managed
  - third-party-managed
- ISIS routing domain subnets
- CPAA

The following figure shows the properties form for an ISIS checkpoint.:

Figure 18-4 ISIS checkpoint



CPAM checkpoint manager

You can use the CPAM checkpoint manager to:

- search for and view specific OSPF or ISIS topology checkpoints
- search for and view checkpointed topology objects, such as routers, IGP links, or subnets
- create topology checkpoints for an administrative domain
- compare checkpoints
- schedule checkpoints

You can create checkpoints by:

- manually using the checkpoint manager
- applying an automatic checkpoint from the OSPF, ISIS, or IGP topology map
- creating a checkpoint schedule policy

A topology object is created as a result of a checkpoint if the object changed since the previous checkpoint. When checkpoints are used for comparisons and IGP history, full topology information is recovered.

Checkpoint schedule policies

You can use the checkpoint manager to schedule checkpoints by creating checkpoint schedule policies. The scheduling function supports the creation of NFM-P-based schedules for the automatic execution of checkpoint tasks at specified times.

You can associate a schedule that you create with a checkpoint scheduled task that can be immediately processed, scheduled for later execution, or retained for future use. A scheduled task must be created in the checkpoint scheduler policy configuration form for the scheduled task. When scheduled tasks are created they are associated with a schedule. A schedule is configurable for one-time or ongoing task execution. You can optionally specify the time at which an ongoing schedule is to stop functioning.

To simplify the creation of NFM-P-based schedules when the user and server are in different time zones, the NFM-P converts and displays schedule times that apply to the user and server. For example, if a user in Chicago needs to schedule a checkpoint scheduled task on a system located in New York, both the user and server local times are displayed. The NFM-P calculates the time difference for the user.

User time zones are configured on the User Preferences form. If a time zone is not configured, the NFM-P uses the time zone of the GUI client. If the time zone is not one of the supported time zone options, the NFM-P displays the time zone ID and uses the GMT time value without the time zone offset.

The NFM-P displays whether daylight savings mode is in effect for the client and server. The daylight saving time is specified for the user start time and is based on the time zone of the user. The daylight savings time does not specify the current time and end time.

Consider the following when you create a checkpoint schedule policy or a scheduled checkpoint task.

- Ensure that scheduled tasks are run sufficiently far apart to allow one task to finish before the next starts. Otherwise, the next occurrence of the task is skipped or delayed if the delay time is configured. There is a minimum time interval of 5 minutes for checkpoint creation. For IGP history, you must choose the appropriate time interval—the shorter interval, the shorter IGP History. Changes are located more precisely in time.
- Do not create schedules that overlap. If a new checkpoint creation overlaps with a previous checkpoint or background cleanup task, the checkpoint will not be created.
- A new scheduled task is shut down by default and must be turned up before it can be run.
- You cannot delete a schedule that has a dependency, for example, one that is associated with a task. To delete and IGP administrative domain Schedule Policy, you must first delete the scheduled task.
- One minute is added to the default start and end time values of a schedule to allow time for schedule configuration.
- A monthly schedule with the Run Every Month or Run Every Months parameter configured uses a 30-day interval.
- When you create a monthly schedule using the Run Every parameter and specify a date that does not exist for the specified months, the last date of the month is used. For example, if you create a monthly scheduled task, starting January 31st, the scheduled task runs on February 28th, March 31st, and April 30th when those months are specified in the schedule.

Checkpoint configuration for IGP history

For the IGP history topology map to be accurate, you must configure the maximumNumberOfCheckpointObjects variable in the nms-server.xml file.

This variable limits the number of topology objects (checkpoints, routers, subnets and links) that are kept in the database to provide IGP history data. The larger this variable, the longer the IGP history is kept and more database space is consumed. Every time the number of objects reaches a threshold, the IGP history background cleanup task begins and removes older objects so that the total number of IGP history objects is lower than the maximumNumberOfCheckpointObjects.

Consider the following steps when you set the maximumNumberOfCheckpointObjects based on network size and stability:

- **1. Calculate the required maximum number using the following formula:**
  Required Maximum Number Of Checkpoint Objects = *#Routers* x (1 + *ExpansionFactor*) x (1 + *PercentChange* x *HoldTime*) x *FluctuationFactor*
  where,
  FluctuationFactor is 3
  #Routers is the number of routers in the network (if a router is part of both OSPF and ISIS, it counts as 2)
  ExpansionFactor is average number of links and subnets per router in the network
  PercentChange is the measure of stability of the network and is equal to (topology object changed)/(total objects) per month. Operational state changes, metrics re-configurations, bandwidth on links etc. are considered changes. Although you cannot precisely predict this parameter, this value is assumed to be 0.1 per month, based on statistical data. This means that in a normal and stable network, 10% of topology objects (routers, subnets, links) are changed.
  HoldTime is the desired time interval in months that a user wants to keep IGP history.
  For example, for the average size network with *#Routers* = 500, *ExpansionFactor* = 10, *PercentChange* = 0.1/month, *HoldTime* = 6 month, the Required Maximum Number Of Checkpoint Objects is 26 400.
- **2. Set maximumNumberOfCheckpointObjects to the larger number of Required Maximum Number Of Checkpoint Objects calculated in step 1, or 50 000.**
  The default value of maximumNumberOfCheckpointObjects is set to 50000 based on the average sized network.
- **3. If the number from step 2 is greater than 100 000, set the maximumNumberOfCheckpointObjects to 100 000.**

18.1.4 Troubleshooting the network by comparing checkpoints

You can use the CPAM to diagnose problems in the network by comparing two checkpoints of the network and viewing the information about the differences in configuration and topology changes. It is also possible to compare a single checkpoint against the current topology rather than a second checkpoint.

When you compare two checkpoints, you can specify whether the comparison is of checkpointed areas, routers, links, or subnets, or a combination of these objects.

You can compare checkpoints from:

- checkpoint manager

- IGP history topology map

When you use the Checkpoint manager to compare checkpoints, you can choose the checkpoints to be compared. When you use the IGP history topology map, the CPAM chooses the two checkpoints in the specified interval that are closest to the start and end dates and times.

The first checkpoint that you select or that is selected by the CPAM in the IGP historical interval is the base for the comparison. You can change the order of the checkpoints so that the second checkpoint that you select becomes the base for the comparison. You can specify a filter to limit the comparison results that are displayed. The CPAM displays a list of the object comparison results, with an entry for each checkpointed object that is compared.

You can view information about the property differences for a specific object, such as a router or link. Differences between the values of a property in the first and second checkpoints are indicated by text, icons, and colors.

Note: See 18.26 “To compare checkpoints” (p. 379) for information about how to compare checkpoints.

The objects involved in an OSPF checkpoint comparison include the following:

- all of the OSPF links in all of the areas
- all of the OSPF routers in all of the areas
- OSPF area subnets and areas

The objects involved in an ISIS checkpoint comparison include the following:

- all of the ISIS links in all of the routing domains
- all of the ISIS routers in all of the routing domains
- ISIS routing domain subnets and areas

18.2 Workflow for impact analysis

18.2.1 Stages

1

As required, perform an IGP impact analysis.

1. Configure a historical IGP impact analysis and the time range for the analysis. See 18.3 “To configure an IGP impact analysis” (p. 348) for more information.
2. Configure IGP history from the IGP topology map. See 18.4 “To configure IGP history from the IGP topology map” (p. 349) for more information.
3. Compare checkpoints on an IGP history topology map. See 18.6 “To compare checkpoints on an IGP history topology map” (p. 353) for more information.

2

As required, perform a BGP impact analysis.

1. Configure the CPAA to register BGP events. See the *7701 CPAA Setup and Installation Guide* for more information.

2. Configure a historical BGP impact analysis. See 18.7 “To configure a historical BGP impact analysis” (p. 358) for more information.
3. Configure the BGP event manager. See 18.8 “To configure the BGP event manager” (p. 360) for more information.
4. Configure the BGP event retrieval. See 18.9 “To configure BGP event retrieval” (p. 360) for more information.

3

As required, perform a VPRN BGP impact analysis. See 18.10 “To configure a VPRN BGP impact analysis” (p. 362) for more information.

4

As required, perform a service impact analysis. See 18.11 “To configure a service impact analysis” (p. 364) for more information.

5

As required, view specific topology changes on an IGP history topology map. See 18.12 “To view specific topology changes on an IGP history topology map” (p. 365) for more information.

6

As required, perform a composite service impact analysis. See 18.13 “To configure a composite service impact analysis” (p. 366) for more information.

7

As required, create and manage checkpoints using the Checkpoint Manager or contextual menu on the topology map.

- Create an OSPF checkpoint for all of the OSPF area within an IGP administrative domain. See 18.14 “To create an OSPF checkpoint” (p. 367) for more information.
- Configure OSPF checkpoints in an IGP administrative domain. See 18.15 “To configure OSPF checkpoints in an IGP administrative domain” (p. 368) for more information.
- Create checkpoints on OSPF areas from an OSPF topology map. See 18.16 “To create checkpoints from an OSPF topology map” (p. 369) for more information.
- Create an ISIS checkpoint for all of the ISIS routing domains within an IGP administrative domain. See 18.17 “To create an ISIS checkpoint” (p. 370) for more information.
- Configure ISIS checkpoints in an IGP administrative domain. See 18.18 “To configure ISIS checkpoints in an IGP administrative domain” (p. 370) for more information.
- Create checkpoints on ISIS routing domains from an ISIS topology map. See 18.19 “To create checkpoints from an ISIS topology map” (p. 371) for more information.
- Create checkpoints on an OSPF area or ISIS routing domain from an IGP topology map. See 18.20 “To create checkpoints from an IGP topology map” (p. 372) for more information.
- Create an administrative domain checkpoint schedule policy, as required. See 18.21 “To create an Admin Domain checkpoint schedule policy” (p. 373) for more information.

- Force delete the IGP history, as required. See 18.22 “To force delete the IGP history” (p. 375) for more information.

8

View the details of impacted IP and paths, LSPs, and affected services. See 18.23 “To view OSPF topology checkpoints” (p. 375) to 18.25 “To view checkpointed topology objects” (p. 377) for more information.

9

Navigate to impacted IP paths, LSPs, and affected services on topology maps.

10

Compare the checkpoints. See 18.26 “To compare checkpoints” (p. 379) for more information.

18.3 To configure an IGP impact analysis

Note: For accurate results, you must ensure that the CPAM and CPAA are administratively up.

18.3.1 Steps

1

Choose Tools→Route Analysis→Impact Analysis from the NFM-P main menu. The Impact Analysis form opens.

2

Click Create and choose IGP Impact Analysis. The IGP Impact Analysis form opens.

3

Click Select and choose an IGP administrative domain.

4

Configure the Time Interval Type parameter.

5

Perform one of the following:

a. If you chose Rewind From/To Interval, configure the Start Time and End Time parameters.

b. If you chose Rewind From Current Time, configure the Time Interval (in minutes) parameter.

c. If you chose Current Status, continue to Step 6 .

6

Click Apply. A list of reasons and statistics for IP paths and LSP paths is displayed.

7

Click Impact Analysis. When the analysis is complete, the lists on the IGP Impact Analysis form show the number of affected IP paths, LSPs, and services.

8

Select an item in a list and click View Impact. The Details: *Reason* form opens.

9

Click on the tabs to view information about path monitors, path records, correlated IGP events, and affected services.

10

Click on the Services tab to view information about the affected services.

11

Close the form.

END OF STEPS

18.4 To configure IGP history from the IGP topology map

Note: For accurate results, you must ensure that the CPAM and CPAA are administratively up.

18.4.1 Steps

1

Choose Tools→Route Analysis→IGP Topology from the NFM-P main menu. The IGP Topology form opens.

2

Right-click on the topology map and choose IGP History from the contextual menu.

3

Choose the IGP topology from the contextual menu. The IGP Graphical History form opens.

4

Configure the Time Interval Type parameter.

5

Perform one of the following:

a. If you selected Rewind From/To Interval, configure the Start Time and End Time parameters.

b. If you selected Rewind From Current Time, configure the Time Interval (in minutes) parameter.

6

Enable the following parameters, as required:

- Configure Link Specific Filters—specifies whether, in the graphical history, the specified link differences and link properties are included. You must enable the Configure Link Specific Filters parameter to configure the filter.

  Note:

  You can choose any combination of link differences and link properties. If you choose more than one difference or property, the CPAM uses an OR filter.

- Include/Exclude All Link Differences — specifies whether all of the differences between the two checkpoints included in the graphical history are included. You must enable the Configure Link Specific Filters option to configure this option and to enable or disable included link differences. This option is enabled by default, and all of the link differences are included.
- Include/Exclude All Link Properties — specifies whether all of the differences between specific properties of the two checkpoints included in the graphical history are listed. You must enable the Configure Link Specific Filters option to configure this option and to enable or disable included link properties. This option is enabled by default, and all of the link properties are included.

When you enable the Configure Link Specific Filters option, you can include or exclude the following link differences:

- Property change and flap
- Property change and added
- Property change and missing
- Missing
- Added
- Property change
- Status flap
- None

When you enable the Configure Link Specific Filters option, you can include or exclude the following link properties:

- Operational state
- Operational state change counter
- Metric
- Metric change counter
- Administrative groups
- Administrative groups change counter
- TE metric
- TE metric change counter
- SRLG values
- SRLG change counter
- Maximum bandwidth (kbps)
- Unreserved bandwidth (Priority 0) (kbps)

- Unreserved bandwidth (Priority 1) (kbps)
- Unreserved bandwidth (Priority 2) (kbps)
- Unreserved bandwidth (Priority 3) (kbps)
- Unreserved bandwidth (Priority 4) (kbps)
- Unreserved bandwidth (Priority 5) (kbps)
- Unreserved bandwidth (Priority 6) (kbps)
- Unreserved bandwidth (Priority 7) (kbps)
- Link ID

7

Click on the OK button. The IGP History Topology map opens.

8

Click on the Impact Analysis button. The Impact Analysis Time Range (Edit) form opens with the following lists:

9

Click on the OK button. The Impact Analysis Time Range (Edit) form opens with the following lists:

- IP path statistics and affected services statistics for:
  - Total number of IP Paths Impacted
  - Total number of IP Paths Re-Routed
  - Total number of IP Paths Failed
  - Total number of IP Paths that have no route
  - Total number of IP Paths that failed auto-OAM
  - Total number of IP Paths that are diverging
  - Total number of IP Paths that lost ECMP
  - Total number of IP Paths that exceeded OAM SLA thresholds
- LSP statistics and affected services statistics for:
  - Total number of LSPs Impacted
  - Total number of LSPs that Re-Routed
  - Total number of LSPs that Failed
  - Total number of LSPs that failed auto-OAM
  - Total number of LSPs that are diverging
  - Total number of LSPs with an active primary
  - Total number of LSPs with an active secondary or standby
  - Total number of LSPs that switched to bypass or detour
  - Total number of LSP Paths that failed
  - Total number of LSP Paths that exceeded OAM SLA thresholds

10

Choose an entry and click on the View Impact button to view specific information about the IP paths or LSPs, and affected services. The Details: *Reason* form opens with the IP Path Monitors tab displayed for IP paths, or the LSP Path Monitors tab displayed for LSPs.

11

Click on the Search button to list the IP paths or LSP paths.

12

Click on the Services tab to view information about the affected services.

13

Close the Details: *Reason* form.

14

Close the Impact Analysis Time Range (Edit) form.

END OF STEPS

18.5 To configure IGP event retrieval

18.5.1 Steps

1

Choose Tools→Route Analysis→Historical Routing Events→IGP→Events from the NFM-P main menu. The IGP Event Retrieval Filter form opens.

2

Click Select and choose an IGP domain.

3

Configure the Time Interval Type parameter.

4

Perform one of the following:

a. If you selected Rewind From/To Interval, configure the Start Time and End Time parameters.

b. If you selected Rewind From Current Time, configure the Time Interval (in minutes) parameter.

5

Configure the Protocol parameter.

6

Click View IGP Events to view IGP events for the specified interval. The *Protocol* Events form opens.

7

Click Search and choose an IGP event. The IGP Link Event form opens.

8

Click on the tabs to view the event details.

The IP Path Record and LSP Path Record tabs show the records that are correlated to the IGP event.

9

Save your changes and close the forms.

END OF STEPS

18.6 To compare checkpoints on an IGP history topology map

18.6.1 Steps

1

Choose Tools→Route Analysis→IGP Topology from the NFM-P main menu. The IGP Topology form opens.

2

Right-click on the topology map and choose IGP History from the contextual menu.

3

Choose the IGP topology from the contextual menu. The IGP Graphical History form opens.

4

Configure the Time Interval Type parameter.

5

Perform one of the following:

a. If you selected Rewind From/To Interval, configure the Start Time and End Time parameters.

b. If you selected Rewind From Current Time, configure the Time Interval (in minutes) parameter.

6

Enable the following parameters, as required:

- Configure Link Specific Filters—specifies whether, in the graphical history, the specified link differences and link properties are included. You must enable the Configure Link Specific Filters parameter to configure the filter.

  Note:

  You can choose any combination of link differences and link properties. If you choose more than one difference or property, the CPAM uses an OR filter.
- Include/Exclude All Link Differences — specifies whether all of the differences between the two checkpoints included in the graphical history are included. You must enable the Configure Link Specific Filters option to configure this option and to enable or disable included link differences. This option is enabled by default, and all of the link differences are included.
- Include/Exclude All Link Properties — specifies whether all of the all of the differences between specific properties of the two checkpoints included in the graphical history are listed. You must enable the Configure Link Specific Filters option to configure this option and to enable or disable included link properties. This option is enabled by default, and all of the link properties are included.

When you enable the Configure Link Specific Filters option, you can include or exclude the following link differences:

- Property change and flap
- Property change and added
- Property change and missing
- Missing
- Added
- Property change
- Status flap
- None

When you enable the Configure Link Specific Filters option, you can include or exclude the following link properties:

- Operational state
- Operational state change counter
- Metric
- Metric change counter
- Administrative groups
- Administrative groups change counter
- TE metric
- TE metric change counter
- SRLG values
- SRLG change counter
- Maximum bandwidth (kbps)
- Unreserved bandwidth (Priority 0) (kbps)
- Unreserved bandwidth (Priority 1) (kbps)
- Unreserved bandwidth (Priority 2) (kbps)
- Unreserved bandwidth (Priority 3) (kbps)
- Unreserved bandwidth (Priority 4) (kbps)

- Unreserved bandwidth (Priority 5) (kbps)
- Unreserved bandwidth (Priority 6) (kbps)
- Unreserved bandwidth (Priority 7) (kbps)
- Link ID

7

Click on the OK button. The IGP History Topology map opens.

8

Right-click on the map and choose Compare.

9

Choose one of the following from the contextual menu:

- OSPF—to compare OSPF checkpoints
  The OSPF - Checkpoint form opens.
- ISIS—to compare ISIS checkpoints
  The ISIS - Checkpoint form opens.

10

Choose a checkpoint A, if necessary. By default, Checkpoint A is configured with the closest checkpoint to the start time within the interval.

1. Click on the Select button next to the Checkpoint A parameter. The Select Object A form opens.
2. Specify a filter for the search, if required, and click on the Search button. A list of checkpoints appears.
3. Select a checkpoint and click on the OK button. The Select Object A form closes.

11

Perform one of the following:

a. Choose a checkpoint B, if necessary. Go to Step 12 .

b. Enable the ...OR Compare With Current Topology checkbox. Go to Step 14 .

12

Choose a checkpoint B, if necessary. By default, Checkpoint B is configured with the closest checkpoint to the end time within the interval.

1. Click on the Select button next to the Checkpoint B parameter. The Select Object B form opens.
2. Specify a filter for the search, if required, and click on the Search button. A list of checkpoints that exist in the same IGP administrative domain as the checkpoint selected for Object A appears.
3. Select a checkpoint entry and click on the OK button. The Select Object B form closes.

13

You can click on the Swap button at any time to change the order of the selected checkpoints. For example, when you click on the Swap button, Checkpoint A becomes Checkpoint B, and Checkpoint B becomes Checkpoint A. Checkpoint B is compared against Checkpoint A.

14

Enable the following parameters, as required:

- Include Only Differences — specifies whether, in a checkpoint comparison operation, only the differences between the two checkpoints being compared are listed.
- Include Only Specified Classes — specifies whether, in a checkpoint comparison operation, only the differences between specific attributes of the two checkpoints being compared are listed.
- Configure Link Specific Filters—specifies whether, in a checkpoint comparison operation, specified link differences and link properties are included in the comparison of the two checkpoints.The Configure Link Specific Filters parameter is configurable only if the Include Only Differences option is disabled. You must enable the Configure Link Specific Filters parameter to configure the filter.
  - Include/Exclude All Link Differences—specifies whether all of the link differences are included or excluded.
  - Include/Exclude All Link Properties—specifies whether all of the link properties are included or excluded.

Note: You can choose any combination of link differences and link properties to be included in the comparison. If you choose more than one difference or property, the CPAM uses an OR filter for the comparison.

When you enable the Include Only Specified Classes option, you can include the following classes in the OSPF checkpoint comparison:

- Area
- OSPF Link
- OSPF Subnet
- Router

When you enable the Include Only Specified Classes option, you can include the following classes in the ISIS checkpoint comparison:

- Area
- ISIS Link
- ISIS Subnet
- Router

When you enable the Configure Link Specific Filters option, you can include or exclude the following link differences in the checkpoint comparison:

- Property change and flap
- Property change and added
- Property change and missing
- Missing
- Added
- Property change
- Status flap
- None

You can enable the Configure Link Specific Filters option only if the Include Only Differences option is disabled.

When you enable the Configure Link Specific Filters option, you can include or exclude the following link properties in the checkpoint comparison:

- Operational state
- Operational state change counter
- Metric
- Metric change counter
- Administrative groups
- Administrative groups change counter
- TE metric
- TE metric change counter
- SRLG values
- SRLG change counter
- Maximum bandwidth (kbps)
- Unreserved bandwidth (Priority 0) (kbps)
- Unreserved bandwidth (Priority 1) (kbps)
- Unreserved bandwidth (Priority 2) (kbps)
- Unreserved bandwidth (Priority 3) (kbps)
- Unreserved bandwidth (Priority 4) (kbps)
- Unreserved bandwidth (Priority 5) (kbps)
- Unreserved bandwidth (Priority 6) (kbps)
- Unreserved bandwidth (Priority 7) (kbps)
- Link ID

You can enable the Configure Link Specific Filters option only if the Include Only Differences option is disabled.

15

Click on the Compare button. A list of differences between the two checkpoints appears. Differences are identified in the Differences column and identified by a color:

- Property Change (blue) — property change to the object identified in the Class Name column
- Missing (pink) — object identified in the Class Name column exists in checkpoint object A and not in checkpoint object B
- Added (green) — object identified in the Class Name column exists in checkpoint object B and not in checkpoint object A

- No change (white) — there are no configuration changes between checkpoint object A and checkpoint object

16

Choose an entry and click on the Properties button to view additional details about the difference. The Difference - Checkpoint (*checkpointed object)object A* to *object B* form appears displaying a list of property changes.

17

Click on an entry to view information about the differences in the panel on the right.

18

Click on the OK button to close the form.

19

Close the Compare - Checkpoint form.

20

Close the IGP History Topology map.

END OF STEPS

18.7 To configure a historical BGP impact analysis

18.7.1 General information

In order to configure a historical BGP impact analysis, the CPAA must first be able to register BGP events. See the *7701 CPAA Setup and Installation Guide* for more information.

18.7.2 Steps

1

Choose Tools→Route Analysis→Impact Analysis from the NFM-P main menu. The Impact Analysis form opens.

2

Click on the Create button and choose BGP Historical Impact Analysis. The BGP Impact Analysis (Create) form opens.

3

Configure the ID and Name parameters.

4

Click on the Select button in the BGP AS Domain panel. The Select Domain - BGP Impact Analysis form opens with a list of BGP AS domains displayed.

5

Choose a domain and click on the OK button. The Select Domain - BGP Impact Analysis form closes and the BGP Impact Analysis (Create) form reappears with the BGP AS Domain information displayed.

6

Configure the Time Interval Type parameter.

7

Perform one of the following:

a. If you selected Rewind From/To Interval, configure the Start Time and End Time parameters.

b. If you selected Rewind From Current Time, configure the Time Interval (in minutes) parameter.

8

Configure the Address Type parameter.

9

If you selected VPN IPv4/VPN IPv6, configure the Type and Route Target parameters.

10

Click on the Apply button. The BGP Historical Impact Analysis (Create) form expands and is renamed as BGP Historical Impact Analysis (Edit).

11

Click on the Impact Analysis button. If the Impact Analysis button is not visible, click on the More Actions button and choose Impact Analysis. The BGP Historical Impact Analysis (Edit) form displays the results of the impact analysis.

12

As required, perform any of the following:

- Click on the View BGP Events button in the Throttled BGP Events panel to view the throttled BGP events.
- Double-click on a prefix event in the Prefix Counter panel to view the details those events.
- Click on the Prefix Analysis button, or on the More Actions button and choose Prefix Analysis, to view the prefix analysis details.
- Click on the Per Next Hop Events Analysis button, or on the More Actions button and choose Per Next Hop Events Analysis, to view the per next hop analysis details.

13

Click on the OK button. A dialog box appears.

14

Click on the Yes button. The BGP Historical Impact (Edit) form closes.

END OF STEPS

18.8 To configure the BGP event manager

18.8.1 General information

In order to configure a historical BGP impact analysis, the CPAA must first be able to register BGP events. See the *7701 CPAA Setup and Installation Guide* for more information.

18.8.2 Steps

1

Choose Tools→Route Analysis→Historical Routing Events→BGP Partition Manager from the NFM-P main menu. The BGP Event Manager form opens with the General tab displayed.

2

Configure the Historical Interval (weeks) and Max BGP Events DB Size (Mbytes) parameters.

3

Click on the BGP Event Partition tab to view event collection statistics for previous intervals.

4

As required, click on the Clear BGP Events button to clear BGP events from the database. If the Clear BGP Events button is not visible, click on the More Actions button and choose Clear BGP Events.

5

Click on the OK button. The BGP Event Manager form closes.

END OF STEPS

18.9 To configure BGP event retrieval

18.9.1 General information

In order to configure a historical BGP impact analysis, the CPAA must first be able to register BGP events. See the *7701 CPAA Setup and Installation Guide* for more information.

18.9.2 Steps

1

Choose Tools→Route Analysis→Historical Routing Events→BGP from the NFM-P main menu. The BGP Event Retrieval Filter form opens.

2

Click Select and choose a BGP AS domain.

3

Configure the Time Interval Type parameter.

4

Perform one of the following:

a. If you selected Rewind From/To Interval, configure the Start Time and End Time parameters.

b. If you selected Rewind From Current Time, configure the Time Interval (in minutes) parameter.

5

Configure the Address Type parameter.

6

If you selected the VPN IPv4/VPN IPv6, EVPN, L2VPN, or MVPN address type, you can enable the Route Distinguisher and Route Target VPN Filters.

7

If you enabled the Route Distinguisher VPN Filter, configure the Route Distinguisher Type and Route Distinguisher parameters.

8

If you enabled the Route Target VPN Filter, configure the Type and Route Target parameters.

9

Click View BGP Events to view BGP events for the specified interval. The BGP Events form opens.

10

Click Search and choose a BGP event. The BGP Prefix Event form opens

11

Review the event details and close the form.

12

Save your changes and close the forms.

END OF STEPS

18.10 To configure a VPRN BGP impact analysis

18.10.1 Steps

1

Perform one of the following:

a. Choose Tools→Route Analysis→Impact Analysis from the NFM-P main menu. The Impact Analysis form opens. Go to Step 6 .

b. Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form appears. Continue to Step 2 .

2

Choose VPRN Service (VPRN) from the object drop-down menu.

3

Configure the filter criteria and click on the Search button. A list of VPRN services appears.

4

Perform one of the following:

a. Select a VPRN service from the list, click on the Impact Analysis button, and choose VPRN BGP. The VPRN BGP Impact Analysis (Create) form opens. Go to Step 7 .

b. Select a VPRN service from the list and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed. Continue to Step 5 .

5

Click on the CPAM button and choose BGP Historical Impact Analysis. The VPRN BGP Historical Impact Analysis form opens.

6

Click on the Create button and choose VPRN BGP Historical Impact Analysis. The VPRN BGP Impact Analysis (Create) form opens.

7

Configure the ID and Name parameters.

8

Click on the Select button in the Service panel. The Select Service - VPRN BGP Impact Analysis form opens with a list of services displayed.

9

Choose a service and click on the OK button. The Select Service - VPRN BGP Impact Analysis form closes and the VPRN BGP Impact Analysis (Create) form reappears with the service information displayed.

10

Click on the Select button in the BGP AS Domain panel. The Select Domain - VPRN BGP Impact Analysis form opens with a list of BGP AS domains displayed.

11

Choose a domain and click on the OK button. The Select Domain - VPRN BGP Impact Analysis form closes and the VPRN BGP Impact Analysis (Create) form reappears with the BGP AS domain information displayed.

12

Configure the Time Interval Type parameter.

13

Perform one of the following:

a. If you selected Rewind From/To Interval, configure the Start Time and End Time parameters.

b. If you selected Rewind From Current Time, configure the Time Interval (in minutes) parameter.

14

Click on the Apply button. The VPRN BGP Impact Analysis (Create) form expands and is renamed as VPRN BGP Impact Analysis (Edit).

15

Click on the Impact Analysis button. If the Impact Analysis button is not visible, click on the More Actions button and choose Impact Analysis. The VPRN BGP Impact Analysis (Edit) form displays the results of the impact analysis.

16

As required, perform any of the following:

- Click on the View BGP Events button in the Throttled BGP Events panel to view the throttled BGP events.
- Double-click on a prefix event in the Prefix Counter panel to view the details those events.
- Click on the Prefix Analysis button, or on the More Actions button and choose Prefix Analysis, to view the prefix analysis details.

- Click on the Per Next Hop Events Analysis button, or on the More Actions button and choose Per Next Hop Events Analysis, to view the per next hop analysis details.
- Click on the View Discovered RD/RT button, or on the More Actions button and choose View Discovered RD/RT, to view all route distinguishers and route targets associated with the VPRN service.

17

Click on the OK button. A dialog box appears.

18

Click on the Yes button. The VPRN BGP Impact Analysis (Edit) form closes.

END OF STEPS

18.11 To configure a service impact analysis

18.11.1 Steps

1

Choose Tools→Route Analysis→Impact Analysis from the NFM-P main menu. The Impact Analysis form opens.

2

Click Create and choose Service IGP Impact Analysis. The Service Impact Analysis form opens.

3

Configure the ID and Name parameters.

4

Select a Service in the Service panel.

5

Configure the Time Interval Type parameter.

6

Perform one of the following:

a. If you selected Rewind From/To Interval, configure the Start Time and End Time parameters.

b. If you selected Rewind From Current Time, configure the Time Interval (in minutes) parameter.

c. If you chose Current Status, continue to Step 8 .

7

Click Apply. A list of reasons and statistics for IP paths and LSP paths is displayed.

8

Click Impact Analysis. When the analysis is complete, the lists on the Service Impact Analysis form show the number of affected IP paths and LSPs or LSP paths.

9

Select an item in a list and click View Impact. The Details: Reason form opens.

10

Click on the tabs to view information about path monitors, path records, and correlated IGP events on the service.

11

Close the forms.

END OF STEPS

18.12 To view specific topology changes on an IGP history topology map

18.12.1 Steps

1

Perform a service impact analysis as described in 18.11 “To configure a service impact analysis” (p. 364) .

2

Perform one of the following:

a. View IGP link events from the Service Impact Analysis form:
   1. Select Total Number of IP Paths Impacted and click Navigate.
   2. Choose *Administrative_Domain*→*Topology_View*→Find Event from the contextual menu. An IGP history topology map opens showing the IGP link event.
   3. Close the IGP history topology map.

b. View IGP link events from the Details: Total Number of IP Paths Impacted form:
   1. Select Total Number of IP Paths Impacted and click View Impact. The Details: Total Number of IP Paths Impacted form opens.
   2. Click on the IGP Event tab.
   3. Select one or more IGP Link Events and click Navigate.

4. Choose *Topology_type→IGP_Administrative_Domain* from the contextual menu. An IGP history topology map opens showing the IGP link event(s).
5. Close the forms.

3

View IP path records:

1. Select Total Number of IP Paths Impacted and click View Impact. The Details: Total Number of IP Paths Impacted form opens.
2. Click on the IP Path monitor records tab.
3. Select an IP Path Record and click Navigate.
4. Choose *Topology_type→IGP_Administrative_Domain* from the contextual menu. An IGP history topology map opens showing the IP path record.
5. Close the forms.

END OF STEPS

18.13 To configure a composite service impact analysis

18.13.1 Steps

1

Choose Tools→Route Analysis→Impact Analysis from the NFM-P main menu. The Impact Analysis form opens.

2

Click on the Create button and choose Composite Service Impact Analysis. The Composite Service Impact Analysis (Create) form opens.

3

Configure the ID and Name parameters.

4

Click on the Select button in the Composite Service panel. The Select Composite Service - Composite Service Impact Analysis form opens with a list of composite services displayed.

5

Choose a composite service and click on the OK button. The Select Composite Service - Composite Service Impact Analysis form closes and the Composite Service Impact Analysis (Create) form reappears with the composite service information displayed.

6

Configure the Time Interval Type parameter.

7

Perform one of the following:

a. If you selected Rewind From/To Interval, configure the Start Time and End Time parameters.

b. If you selected Rewind From Current Time, configure the Time Interval (in minutes) parameter.

c. If you chose Current Status, continue to Step 8 .

8

Click on the OK button. A dialog box appears.

9

Click on the Yes button. The Composite Service Impact Analysis (Create) form closes.

END OF STEPS

18.14 To create an OSPF checkpoint

18.14.1 Steps

1

Choose Tools→Route Analysis→Checkpoints from the NFM-P main menu. The Checkpoint Manager form opens.

2

Click on the Create button and choose OSPF Checkpoint from the contextual menu. The OSPF Checkpoint (Create) form opens.

3

Click on the Select button next to the Domain ID parameter. The Select IGP Domain - OSPF Checkpoint form opens.

4

Choose an entry and click on the OK button. The Select IGP Domain - OSPF Checkpoint form closes and the OSPF Checkpoint (Create) form refreshes with the IGP administrative domain information.

5

Configure the parameters:

- Name
- Description

6

Click on the OK button. The OSPF Checkpoint (Create) form closes.

7

Close the Checkpoint Manager form.

END OF STEPS

18.15 To configure OSPF checkpoints in an IGP administrative domain

18.15.1 Steps

1

Choose Tools→Route Analysis→Checkpoints from the NFM-P main menu. The Checkpoint Manager form opens.

2

Click the Select Object Type button and click on IGP Administrative Domain (CPAM: Topology).

3

Specify a filter for the search, if required, and click on the Search button. A list of IGP administrative domains appears.

4

Choose an entry and click on the Properties button. The IGP Administrative Domain (Edit) form appears with the General tab displayed.

5

Click on the Checkpoints tab. The OSPF tab is displayed.

6

Perform one of the following:

a. Add an OSPF checkpoint to the IGP administrative domain.
   1. Click on the Add button. The OSPF Checkpoint (Create) form opens.
   2. Configure the parameters:
      - Name
      - Description
   3. Click on the OK button. The OSPF Checkpoint (Create) form closes.

b. Modify an OSPF checkpoint in the IGP administrative domain.
   1. Select an OSPF checkpoint and click on the Properties button. The OSPF Checkpoint (Edit) form opens with the General tab displayed.
   2. Configure the parameters:

- Name
- Description

3. Click on the OK button. The OSPF Checkpoint (Edit) form closes.

c. Remove an OSPF checkpoint from the IGP administrative domain.

1. Select one or more OSPF checkpoints and click on the Delete button. A dialog box appears.
2. Click on the Yes button. The dialog box closes and the OSPF checkpoint is removed.

7

Close the IGP Administrative Domain (Edit) form.

8

Close the Checkpoint Manager form.

Note: See 18.21 “To create an Admin Domain checkpoint schedule policy” (p. 373) for information about how to schedule checkpoints.

END OF STEPS

18.16 To create checkpoints from an OSPF topology map

18.16.1 Steps

1

Choose Tools→Route Analysis→OSPF Topology→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate OSPF topology map opens.

2

Right-click on the map and choose Checkpoint from the contextual menu.

3

Perform one of the following:

a. Choose All OSPF Areas from the contextual menu to create checkpoints for every OSPF area in the IGP administrative domain.

b. Choose Checkpoint Manager from the contextual menu. The Checkpoint Manager form opens.

4

Close the topology map.

END OF STEPS

18.17 To create an ISIS checkpoint

18.17.1 Steps

1

Choose Tools→Route Analysis→Checkpoints from the NFM-P main menu. The Checkpoint Manager form opens.

2

Click on the Create button and choose ISIS Checkpoint from the contextual menu. The ISIS Checkpoint (Create) form opens.

3

Configure the parameters:

- Name
- Description

4

Click on the OK button. The ISIS Checkpoint (Create) form closes.

5

Close the Checkpoint Manager form.

END OF STEPS

18.18 To configure ISIS checkpoints in an IGP administrative domain

18.18.1 Steps

1

Choose Tools→Route Analysis→Checkpoints from the NFM-P main menu. The Checkpoint Manager form opens.

2

Choose IGP Administrative Domain (CPAM: Topology) from the object drop-down menu.

3

Specify a filter for the search, if required, and click on the Search button. A list of IGP administrative domains appears.

4

Choose an entry and click on the Properties button. The IGP Administrative Domain (Edit) form appears with the General tab displayed.

5

Click on the Checkpoints tab. The OSPF tab is displayed.

6

Perform one of the following:

a. Add an ISIS checkpoint to the IGP administrative domain.
   1. Click on the ISIS tab.
   2. Click on the Add button. The ISIS Checkpoint (Create) form opens.
   3. Configure the parameters:
      - Name
      - Description
   4. Click on the OK button. The ISIS Checkpoint (Create) form closes.

b. Modify an ISIS checkpoint in the IGP administrative domain.
   1. Select an ISIS checkpoint and click on the Properties button. The ISIS Checkpoint (Edit) form opens with the General tab displayed.
   2. Configure the parameters:
      - Name
      - Description
   3. Click on the OK button. The ISIS Checkpoint (Edit) form closes.

7

Close the IGP Administrative Domain (Edit) form.

8

Close the Checkpoint Manager form.

Note: See 18.21 “To create an Admin Domain checkpoint schedule policy” (p. 373) for information about how to schedule checkpoints.

END OF STEPS

18.19 To create checkpoints from an ISIS topology map

18.19.1 Steps

1

Choose Tools→Route Analysis→ISIS Topology→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate ISIS topology map opens.

2

Right-click on the map and choose Checkpoint from the contextual menu.

3

Perform one of the following:

a. Choose All ISIS Domains from the contextual menu to create checkpoints for every ISIS routing domain in the IGP administrative domain.

b. Choose Checkpoint Manager from the contextual menu. The Checkpoint Manager form opens.

4

Close the topology map.

END OF STEPS

18.20 To create checkpoints from an IGP topology map

18.20.1 Steps

1

Choose Tools→Route Analysis→IGP Topology→*IGP_Administrative_Domain* from the NFM-P main menu. The appropriate IGP topology map opens.

2

Right-click on the map and choose Checkpoint from the contextual menu.

3

Perform one of the following:

a. Choose All OSPF Areas from the contextual menu to create checkpoints for every OSPF area in the IGP administrative domain.

b. Choose All ISIS Domains from the contextual menu to create checkpoints for every ISIS routing domain in the IGP administrative domain.

c. Choose All from the contextual menu to create checkpoints for all of the ISIS routing domains and OSPF areas in the IGP administrative domain.

d. Choose Checkpoint Manager from the contextual menu. The Checkpoint Manager form opens.

4

Close the topology map.

END OF STEPS

18.21 To create an Admin Domain checkpoint schedule policy

18.21.1 Steps

1

Choose Tools→Route Analysis→Checkpoints from the NFM-P main menu. The Checkpoint Manager form opens.

Note: Alternatively, you can create a checkpoint schedule policy from the IGP administrative domain. Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.
Click on the Search button and choose an IGP administrative domain. Click on the Properties button. The IGP Administrative Domain (Edit) form appears with the General tab displayed.
Click on the Checkpoints tab. The OSPF tab is displayed. Click on the ISIS Schedule Policies tab.
Click on the Add button. The ISIS Checkpoint Schedule Policy (Create) form opens. Go to Step 5 .

2

Click on the Create button and choose Admin Domain Checkpoint Schedule from the contextual menu. The Checkpoint Schedule Policy (Create) form opens.

3

Click on the Select button next to the Domain Number. The Select IGP Admin Domain - Checkpoint Schedule Policy form opens.

4

Choose an entry and click on the OK button. The Select IGP Admin Domain - Checkpoint Schedule Policy form closes.

5

Configure the parameters:

- Name
- Description

6

Perform one of the following:

a. Click on the OK button to save the configuration and close the Admin Domain Checkpoint Schedule Policy (Create) form.

b. Click on the Apply button and perform Step 7 to Step 11 to associate a checkpoint scheduled task with the checkpoint schedule policy.

7

Click on the Schedule button and choose Create Checkpoint Scheduled Task from the contextual menu. The Checkpoint Scheduled Task (Create) form opens.

8

Configure the parameters:

- Scheduled Task Name
- Scheduled Task Description
- Administrative State

9

Click on the Select button next to the ID parameter. The Select Schedule - Checkpoint Scheduled Task form opens.

10

Perform one of the following:

a. Select an existing scheduled task and click on the OK button. The Select Schedule - Checkpoint Scheduled Task form closes.

b. Create a scheduled task by performing the following steps.

1. Click on the Create button. The NFM-P Schedule (Create) form opens with the General tab displayed.
2. Configure the parameters:

   - Name
   - Description
   - User Start Time
   - User End Time
   - Ongoing
   - Enable
   - Delay Time (seconds)
   - Frequency

   The User End Time parameter is configurable when the Ongoing parameter is disabled and the Frequency parameter value is set to something other than Once.

   When an NFM-P Schedule is not Ongoing and is assigned to a task, The NFM-P raises an alarm when the User End Time expires.

   Note:

   The checkpoint scheduler can run at an interval of no less than 5 minutes.

3. Click on the OK button. The NFM-P Schedule (Create) form closes and the Select Schedule - Checkpoint Scheduled Task form reappears.
4. Select the schedule you created and click on the OK button. The Select Schedule - Checkpoint Scheduled Task form closes.

11

Click on the OK button. The Checkpoint Scheduled Task (Create) form closes.

12

Close the Checkpoint Manager form.

END OF STEPS

18.22 To force delete the IGP history

18.22.1 When to use

Perform this procedure only in the case of an invalid checkpoint configuration or software problems. This procedure performs a complete checkpoint cleanup for all of the administrative domains, all of the checkpoint objects are deleted, and IGP history is lost.

18.22.2 Steps

1

Choose Tools→Route Analysis→Checkpoints from the NFM-P main menu. The Checkpoint Manager form opens.

2

Click on the Force Delete from the contextual menu. A dialog box appears.

3

Click on the Yes button. All checkpoints are removed from the systems and IGP history is lost.

END OF STEPS

18.23 To view OSPF topology checkpoints

18.23.1 Steps

1

Choose Tools→Route Analysis→Checkpoints from the NFM-P main menu. The Checkpoint Manager form opens.

2

Choose OSPF Checkpoint (CPAM: Topology) from the object drop-down menu.

3

Click on the Search button. A list of OSPF checkpoints appears.

4

Choose an entry and click on the Properties button. The OSPF Checkpoint (Edit) form opens with the General tab displayed.

5

View the following information:

- IGP administrative domain
- checkpoint ID
- checkpoint timestamp
- OSPF area ID
- user that created the checkpoint

6

Configure the parameters, if required:

- Name
- Description

7

Click on the Faults tab to view the alarms for the checkpoint.

8

Click on the OK button to save the changes or on the Cancel button to close the form. A dialog box appears.

9

Click on the Yes button. The OSPF Checkpoint (Edit) form closes.

10

Close the Checkpoint Manager form.

END OF STEPS

18.24 To view ISIS topology checkpoints

18.24.1 Steps

1

Choose Tools→Route Analysis→Checkpoints from the NFM-P main menu. The Checkpoint Manager form opens.

2

Choose ISIS Checkpoint (CPAM: Topology) from the object drop-down menu.

3

Click on the Search button. A list of ISIS checkpoints appears.

4

Choose an entry and click on the Properties button. The ISIS Checkpoint (Edit) form opens with the General tab displayed.

5

View the following information:

- IGP administrative domain
- checkpoint ID
- checkpoint timestamp
- ISIS level
- CPAA IP address
- user that created the checkpoint

6

Configure the parameters, if required:

- Name
- Description

7

Click on the Faults tab to view the alarms for the checkpoint.

8

Click on the OK button to save the changes or on the Cancel button to close the form. A dialog box appears.

9

Click on the Yes button. The ISIS Checkpoint (Edit) form closes.

10

Close the Checkpoint Manager form.

END OF STEPS

18.25 To view checkpointed topology objects

18.25.1 General information

Perform this procedure to view checkpointed topology objects. The checkpointed objects are contained within an OSPF or ISIS checkpoint and represent real objects that existed in the network at a specific time.

18.25.2 Steps

1

Choose Tools→Route Analysis→Checkpoints from the NFM-P main menu. The Checkpoint Manager form opens.

2

Choose one of the following objects from the object drop-down menu:

- **Area (CPAM: Topology)**
  Checkpoints of an area
- **IGP Link (CPAM: Topology)**
  Checkpointed IGP link
- **Router (CPAM: Topology)**
  Checkpoints of a router within an IGP administrative domain
- **Subnet (CPAM: Topology)**
  Checkpoints of a subnet within an IGP administrative domain

3

Click on the Search button. A list of checkpointed objects appears.

4

Choose an entry and click on the Properties button. The *Object* Checkpoint (Edit) form appears.

5

Configure the parameters:

- Name
- Description

The Name parameter is configurable only for checkpointed routers.

6

Click on the Checkpoint Details tab to view the following information about the checkpoint:

- IGP administrative domain
- checkpoint protocol—ISIS or OSPF
- checkpoint ID
- checkpoint time

7

Click on the Faults tab to view alarm information.

8

The tabs that appear depend on the checkpointed object that you are viewing. Click on the tabs to view information about the checkpointed object:

- originating links
- areas
- traffic engineering
- administrative groups

9

Click on the OK button. The *Object* Checkpoint (Edit) form closes.

10

Close the Checkpoint Manager form.

END OF STEPS

18.26 To compare checkpoints

18.26.1 General information

Perform this procedure to compare two checkpoints. The checkpointed objects must be in the same IGP administrative domain, in the same protocol, and in the same routing domain (OSPF area or ISIS routing domain).

18.26.2 Steps

1

Choose Tools→Route Analysis→Checkpoints from the NFM-P main menu. The Checkpoint Manager form opens.

2

Click on the Compare button. The Compare - Checkpoint form opens.

3

Click on the Select button next to the Checkpoint A parameter. The Select Object A form opens.

4

Perform one of the following:

a. Choose ISIS Checkpoint (CPAM: Topology) from the object drop-down menu to compare ISIS checkpoints.

b. Choose OSPF Checkpoint (CPAM: Topology) from the object drop-down menu to compare OSPF checkpoints.

5

Specify a filter for the search, if required, and click on the Search button. A list of checkpoints appears.

6

Select a checkpoint and click on the OK button. The Select Object A form closes.

7

Perform one of the following:

a. Click on the Select button next to the Checkpoint B parameter. The Select Object B form opens. Go to Step 8 .

b. Enable the ...OR Compare With Current Topology checkbox. Go to Step 11 .

8

Specify a filter for the search, if required, and click on the Search button. A list of checkpoints that exist in the same IGP administrative domain as the checkpoint selected for Object A appears.

9

Select a checkpoint entry and click on the OK button. The Select Object B form closes.

10

You can click on the Swap button at any time to change the order of the selected checkpoints. For example, when you click on the Swap button, Checkpoint A becomes Checkpoint B, and Checkpoint B becomes Checkpoint A. Checkpoint B is compared against Checkpoint A.

11

Enable the following parameters, as required:

- Include Only Differences — specifies whether, in a checkpoint comparison operation, only the differences between the two checkpoints being compared are listed.
- Include Only Specified Classes — specifies whether, in a checkpoint comparison operation, only the differences between specific attributes of the two checkpoints being compared are listed.
- Configure Link Specific Filters—specifies whether, in a checkpoint comparison operation, specified link differences and link properties are included in the comparison of the two checkpoints.The Configure Link Specific Filters parameter is configurable only if the Include Only Differences option is disabled. You must enable the Configure Link Specific Filters parameter to configure the filter.
  - Include/Exclude All Link Differences—specifies whether all of the link differences are included or excluded.
  - Include/Exclude All Link Properties—specifies whether all of the link properties are included or excluded.

Note: You can choose any combination of link differences and link properties to be included in the comparison. If you choose more than one difference or property, the CPAM uses an OR filter for the comparison.

When you enable the Include Only Specified Classes option, you can include the following classes in the OSPF checkpoint comparison:

- Area
- OSPF Link
- OSPF Subnet
- Router

When you enable the Include Only Specified Classes option, you can include the following classes in the ISIS checkpoint comparison:

- Area
- ISIS Link
- ISIS Subnet
- Router

When you enable the Configure Link Specific Filters option, you can include or exclude the following link differences in the checkpoint comparison:

- Property change and flap
- Property change and added
- Property change and missing
- Missing
- Added
- Property change
- Status flap
- None

You can enable the Configure Link Specific Filters option only if the Include Only Differences option is disabled.

When you enable the Configure Link Specific Filters option, you can include or exclude the following link properties in the checkpoint comparison:

- Operational state
- Operational state change counter
- Metric
- Metric change counter
- Administrative groups
- Administrative groups change counter
- TE metric
- TE metric change counter
- SRLG values
- SRLG change counter
- Maximum bandwidth (kbps)
- Unreserved bandwidth (Priority 0) (kbps)
- Unreserved bandwidth (Priority 1) (kbps)

- Unreserved bandwidth (Priority 2) (kbps)
- Unreserved bandwidth (Priority 3) (kbps)
- Unreserved bandwidth (Priority 4) (kbps)
- Unreserved bandwidth (Priority 5) (kbps)
- Unreserved bandwidth (Priority 6) (kbps)
- Unreserved bandwidth (Priority 7) (kbps)
- Link ID

You can enable the Configure Link Specific Filters option only if the Include Only Differences option is disabled.

12

Click on the Compare button. A list of differences between the two checkpoints appears. Differences are identified in the Differences column and identified by a color:

- Property Change (blue) — property change to the object identified in the Class Name column
- Missing (pink) — object identified in the Class Name column exists in checkpoint object A and not in checkpoint object B
- Added (green) — object identified in the Class Name column exists in checkpoint object B and not in checkpoint object A
- No change (white) — there are no configuration changes between checkpoint object A and checkpoint object

13

Choose an entry and click on the Properties button to view additional details about the difference. The Difference - Checkpoint (*checkpointed object)object A* to *object B* form appears displaying a list of property changes.

14

Click on an entry to view information about the differences in the panel on the right.

15

Click on the OK button to close the form.

16

Close the Compare - Checkpoint form.

17

Close the Checkpoint Manager form.

END OF STEPS

19 Impact analysis simulation

19.1 Impact analysis simulation overview

19.1.1 Introduction

The CPAM allows you to create a simulated network topology to test the impact of changes to the simulated network on existing IP paths. An IP path represent one or more GRE or LDP tunnels of the same source and destination. In addition, the CPAM supports RSVP LSP simulation.

The simulated topology—or scenario—can be an OSPF or ISIS network in an IGP administrative domain. The simulated network allows you to analyze the impact of typical network changes, such as the following:

- changes to the status of a router, such as:
  - turn up
  - shutdown
  - add
  - delete (not recommended)
- changes to the status of a link, such as:
  - turn up
  - shutdown
  - add
  - delete (not recommended)
- changes to the configuration of a link, such as:
  - total bandwidth and available bandwidth
  - administrative groups
  - metric (cost)
  - changes to LSP measured bandwidth, to see impacts on link utilization

The simulated topology has four modes of operation that are indicated in the top-left corner of the topology map:

- Topology being modified (yellow indicator)

  The topology is in this mode of operation when a change is made to the topology.
- Analyzing impact (blue indicator)

  The topology is in this mode of operation when you click on the Impact Analysis button after modifying the topology, and indicates that the CPAM is analyzing the topology changes and determining the impact on path monitors.
- Topology converged (grey indicator)

  The topology is in this mode of operation after an impact analysis has been performed. You can perform SPF and CSPF highlight operations only when the topology is in this mode of operation.
- Importing (blue indicator)

  The topology is in this mode of operation when you import objects into the impact analysis scenario.

When you change a network object attribute, or add or delete a simulated object, the operation mode indicator on the simulated topology changes from *Topology converged* to *Topology being modified*. When the topology is converged after you start the impact analysis by clicking on the Impact Analysis button, you can perform the following functions on the converged topology:

- calculate SPF
- calculate CSPF
- monitor IP paths

You can create a scenario manually, or populate a scenario from a checkpoint, the real network, or from an existing scenario. Only two scenario sessions can be active at the same time. You need the topology simulation scope of command to use the impact analysis manager.

19.2 MPLS model simulation

19.2.1 General information

An LSP path is a binding of an LSP to a provisioned path. An LSP path is either primary or secondary within the context of the parent LSP. The CPAM MPLS simulation model allows you to configure, monitor, and investigate the impact of the creation and removal of LSP configurations, in addition to the interaction between several LSPs.

The MPLS simulation allows you to determine which LSPs are impacted by topology changes—such as changes to metrics, operational state, bandwidth, or administrative groups—and to determine how different LSPs with conflicting bandwidth requirements interact. You can also configure changes to the measured bandwidth of individual LSPs, to see the impact on link utilization. The simulated MPLS model maintains a history of the actual path of the LSP.

When you create an MPLS scenario, you can import NFM-P dynamic LSPs and their primary and secondary LSP paths. In addition, simulated LSPs in one scenario can be imported into another scenario. You cannot import CPAM LSP path monitors into an MPLS scenario.

You can assign a processing order to each LSP in the simulation. The CPAM first processes the LSPs with a lower processing order. LSPs with equal processing orders are handled one at a time in a non-deterministic order. For example, the following LSPs are configured in the network with the assigned processing priority:

- LSP A (processing order 1)
- LSP B (processing order 2)
- LSP C (processing order 2)

The simulator first processes LSP A. If LSP A results in any bandwidth reservations, the bandwidth reservations are recorded. Next, the simulator processes either LSP B or C.

19.2.2 Point-to-point LSP

The CPAM LSP is a simulation of the NFM-P LSP. The LSP has a single primary LSP path and multiple secondary LSP paths. Secondary paths may be standby paths. The simulated LSP allows you to monitor the active path of the LSP, to determine whether a primary or secondary path is used, or to determine whether a non-standby path should be made active. A history of the active paths is stored. You can highlight any historical active path on a topology map.

19.2.3 LSP paths

An LSP path represents a single simulated provisioned path contained within an LSP. The provisioned path, like the real LSP paths, has zero or more configured loose or strict hops. Historical path results are stored for the LSP path. You can highlight any historical actual path or potential actual path, or the provisioned path on a topology map.

When the simulated IGP topology is converged, you can perform a resignalling of the LSP so that the CPAM rebuilds the LSP path.

The following is the active path selection process:

- Primary path is used.
- If the primary path cannot be setup or is preempted, an operationally enabled secondary standby path is used.
- If there is no operationally enabled secondary standby paths, an attempt is made to setup other secondary paths.
- Each time we resignal and the active path is not the primary path, the simulator attempts to revert back to the primary path.

19.2.4 Non-constraint LSP path

An LSP path without CSPF enabled follows the normal IGP shortest path. If there is a topology change, the LSP path may be impacted and be rerouted (including optimization) or go down. The simulator evaluates during impact analysis, and immediately reroutes the LSP path, if necessary.

19.2.5 Importing paths into the simulation

When you create a scenario and start the simulator for the first time, and import the topology from the live network, you can import all or selected LSP paths and IP path monitors from the real network. The CPAM simulator imports the selected LSP paths and IP path monitors when the topology is imported.

For LSPs, the CPAM also imports the actual paths. If the CPAM cannot map a segment of the actual path to a simulator IGP link during the import, the segment is not imported.

19.3 Workflow for impact analysis simulation

19.3.1 Stages

1

Create a scenario or open an existing scenario. See 19.4 “To create a scenario” (p. 387) and 19.5 “To open a scenario” (p. 391) for more information.

2

Start the simulation. See 19.4 “To create a scenario” (p. 387) for more information.

3

Import objects.

- Import MPLS objects from the NFM-P network. See 19.28 “To import MPLS objects from the NFM-P” (p. 423) for more information.
- Import IP paths from other scenarios or from the NFM-P network. See 19.29 “To import IP paths” (p. 425) for more information.

4

Manage objects on the simulated IGP topology view.

- Add routers. See 19.7 “To create a simulated OSPF router” (p. 393) and 19.11 “To create a simulated ISIS router” (p. 398) for more information.
- Add links. See 19.9 “To add a simulated OSPF link” (p. 395) , 19.10 “To add a simulated OSPF virtual link” (p. 397) , and 19.13 “To add a simulated ISIS link” (p. 400) for more information.ee Procedures
- Add subnets. See 19.8 “To create a simulated OSPF subnet” (p. 394) and 19.12 “To create a simulated ISIS subnet” (p. 399) for more information.
- View and configure areas, routing domains, routers, links, or subnets. See 19.15 “To view and configure a simulated OSPF area” (p. 404) to 19.23 “To view and configure a simulated ISIS router” (p. 413) for more information.
- Turn up or shut down routers, links, or subnets. See 19.24 “To change the administrative state of a simulated network object” (p. 414) for more information.
- Create provisioned paths. See 19.25 “To create a simulated provisioned MPLS path” (p. 415) for more information.
- Create LSPs. See 19.26 “To create a simulated LSP” (p. 417) for more information.
- View historical LSP path records. See 19.30 “To view historical LSP path records” (p. 426) for more information.
- Perform a manual resignal of an LSP. See 19.31 “To perform a manual resignal of an LSP” (p. 428) for more information.
- Capture the path of LSP associated with an LSP. See 19.32 “To capture the path of LSP paths associated with an LSP” (p. 429) for more information.
- Monitor simulated IP paths. See 19.33 “To monitor a simulated IP path” (p. 430) for more information.
- Delete simulated objects. See 19.34 “To delete a simulated network object” (p. 431) for more information.

5

View configuration information about simulated network objects in a scenario. See 19.14 “To view simulated IGP network data” (p. 402) for more information.

6

Highlight objects, as required.

- Highlight simulated LSPs. See 19.35 “To highlight a simulated LSP” (p. 432) for more information.
- Highlight historical simulated LSP path records. See 19.36 “To highlight a simulated historical LSP path record” (p. 433) for more information.
- Highlight simulated LSP paths. See 19.37 “To highlight a simulated LSP path” (p. 434) for more information.
- Highlight SPF links. See 19.38 “To highlight SPF links” (p. 435) for more information.
- Highlight CSPF. See 19.39 “To highlight CSPF” (p. 436) for more information.
- Highlight historical simulated IP path records. See 19.40 “To highlight a historical simulated IP path record” (p. 439) for more information.

7

View the history of simulation events. See 19.41 “To view the history of simulation events” (p. 440) for more information.

8

Manage impact analysis sessions. See 19.42 “To manage impact analysis sessions” (p. 441) for more information.

19.4 To create a scenario

Note: Nokia recommends that you create a scenario for each network that you want to simulate. You cannot roll back changes.

19.4.1 Steps

1

Choose Tools→Route Analysis→Simulated Impact Analysis from the NFM-P main menu. The Simulated Impact Analysis form opens.

2

Click on the Create Scenario button. The Scenario (Create) form opens with the General tab displayed.

3

Configure the parameters:

- Scenario Name
- Description

4

Click on the IGP Topology tab button.

5

Configure the IGP Protocol parameter.

Note: You can specify only one IGP protocol for the impact analysis simulation.

6

Click on the MPLS Topology tab button.

7

Configure the Administrative State parameter.

8

Click on the Apply button.

9

Click on the Start Simulation button. The Creating a new IGP topology form opens.

10

Perform one of the following:

a. Create an empty topology:
   1. Select the Create an empty topology option.
   2. Click on the OK button. The Creating a new IGP topology form closes and the SIMULATION - IGP Model - Scenario topology map opens.
   3. Go to Step 12 .

b. Import a topology from an existing IGP administrative domain:
   1. Select the Import topology from an IGP Admin Domain option.
   2. Click on the Select button in the Import topology from an IGP Admin Domain panel. The Select IGP Administrative Domain form opens.
   3. Click on the Search button. A list of IGP administrative domains appears.
   4. Choose an IGP administrative domain and click on the OK button. The Select IGP Administrative Domain form closes and the Creating a new IGP topology form refreshes with the IGP administrative domain information.
   5. Specify whether you want to import LSPs. Choose one of the following:
      - Import All LSPs
      - Import Selected LSPs
   6. If you select Import Selected LSPs, click on the Selected LSP tab button. Otherwise, go to 11 .
   7. Click on the Add button. The Select... form opens.

8. Click on the Search button. A list of LSPs appears.
9. Choose one or more LSPs and click on the OK button. The Select... form closes.
10. Click on the Import tab button.
11. Specify whether you want to import IP monitored paths. Choose one of the following:
    - Import All IP
    - Import Selected IP Monitored Path
12. If you select Import Selected IP monitored paths, click on the Selected IP tab button. Otherwise, go to 16 .
13. Click on the Add button. The Select... form opens.
14. Click on the Search button. A list of IP monitored paths appears.
15. Choose one or more IP monitored paths and click on the OK button. The Select... form closes.
16. Click on the Import button. The Creating a new IGP topology form closes and the Scenario (Edit) form appears.

c. Import a topology from an existing scenario:
   1. Select the Import topology from another scenario option.
   2. Click on the Select button in the Import topology from another scenario panel. The Select... form opens.
   3. Click on the Search button. A list of scenarios appears.
   4. Choose an entry and click on the OK button. The Select... form closes and the Creating a new IGP topology form refreshes with the scenario information.
   5. Click on the Import button. The Creating a new IGP topology form closes and the Scenario (Edit) form reappears.
   6. Go to Step 11 .

d. Import a topology from a checkpoint:
   1. Select the Import topology from a checkpoint option.
   2. Click on the Select button in the Import topology from a checkpoint panel. The Select... form opens.
   3. Click on the Search button. A list of checkpoints appears.
   4. Choose an entry and click on the OK button. The Select... form closes and the Creating a new IGP topology form refreshes with the checkpoint information.
   5. Click on the Import button. The Creating a new IGP topology form closes and the Scenario (Edit) form reappears.
   6. Go to Step 11 .

e. Import a topology from an OSPF area:
   1. Select the Import topology from an OSPF Area option.
   2. Click on the Select button in the Import topology from an OSPF Area panel. The Select... form opens.
   3. Click on the Search button. A list of OSPF areas appears.

4. Choose an entry and click on the OK button. The Select... form closes and the Creating a new IGP topology form refreshes with the OSPF area information.
5. Click on the Import button. The Creating a new IGP topology form closes and the Scenario (Edit) form reappears.
6. Go to Step 11 .

f. Import a topology from an ISIS routing domain:

1. Select the Import topology from an ISIS Routing Domain option.
2. Configure the Level parameter.
3. Click on the Select button in the Import topology from an ISIS Routing Domain panel. The Select... form opens.
4. Click on the Search button. A list of CPAAs appears.
5. Choose an entry and click on the OK button. The Select... form closes and the Creating a new IGP topology form refreshes with the CPAA information.
6. Click on the Import button. The Creating a new IGP topology form closes and the Scenario (Edit) form reappears.

11

Perform the following to start the simulation:

1. Click on the IGP Topology View button. The Scenario (Edit) form closes and the SIMULATION - IGP Model - Scenario topology map opens.
2. Double-click on the Discovered Vertices object on the topology map. The Discovered L3 Objects form opens with the Routers tab displayed.

   Note:

   Any groups that are configured on the source topology map—OSPF Topology or ISIS Topology—are also imported. Any routers or subnets in the groups on the source topology map appear after the import.

   The OSPF virtual links are imported only if the transit area is visible in the IGP domain (a CPAA is connected to the transit area).

   Because checkpoints contain a single area, virtual links are not imported because the transit area is not visible.
3. Select all of the entries in the list, and drag and drop them on to the topology map.
4. Return to the Discovered L3 Objects form and click on the Subnets tab button.
5. Select all of the entries in the list, and drag and drop them on to the topology map.
6. Click on the Auto-layout button, if required. A dialog box appears.
7. Click on the Yes button. The dialog box closes.

12

Click on the Impact Analysis button on the SIMULATION - IGP Model - Scenario topology map to run the analysis. The Legend - SIMULATION - IGP Model - Scenario form opens with the Last Impact Results tab displayed. When the impact analysis is complete, Topology Converged is displayed.

Note: For quick reference to the last results of the impact analysis, you can keep the Legend - SIMULATION - IGP Model - Scenario form open while you are working with the simulation topology.

13

Click on the View Impact Details button, if required, to view the details of the impact analysis. The Action Event - Impact Analysis - SIMULATION - Scenario (Edit) form opens with the General tab displayed.

14

Click on the following tabs to view information about the impact analysis simulation:

- Attributes
- Scenario
- IP Paths
- LSP Paths
- Services

15

Close the Action Event - Impact Analysis - SIMULATION - Scenario (Edit) form.

16

Click on the Close button to close the Legend - SIMULATION - IGP Model - Scenario form.

17

Close the SIMULATION - IGP Model - Scenario topology map.

18

Close the Simulated Impact Analysis form.

END OF STEPS

19.5 To open a scenario

19.5.1 Steps

1

Choose Tools→Route Analysis→Simulated Impact Analysis from the NFM-P main menu. The Simulated Impact Analysis form opens.

2

Specify a filter for the search, if required, and click on the Search button.

3

Choose an entry and click on the Properties button. The Scenario (Edit) form opens with the General tab displayed.

4

Click on the IGP Topology button. The SIMULATION - IGP Model - Scenario topology map opens.

Note: If the IGP Topology button is disabled, click on the Start Simulation button to enable it.

END OF STEPS

19.6 To view the status of an import

19.6.1 Steps

1

Choose Tools→Route Analysis→Simulated Impact Analysis from the NFM-P main menu. The Simulated Impact Analysis form opens.

2

Specify a filter for the search, if required, and click on the Search button.

3

Choose an entry and click on the Properties button. The Scenario (Edit) form opens with the General tab displayed.

4

View the Import State in the State panel:

- New
- Import Completed

- Importing Igp Domain
- Importing from Another Scenario
- Importing from checkPoint
- Importing from OSPF Area
- Importing from ISIS Level
- Import Completed
- Failed
- Topology Imported
- Importing LSP Paths
- LSP Imported
- Importing IP Paths
- IP Imported

5

Close the Scenario (Edit) form.

END OF STEPS

19.7 To create a simulated OSPF router

19.7.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on the map and choose Add→Router from the contextual menu. The Simulated Router (Create) form opens with the General tab displayed.

3

Configure the parameters:

- Router ID
- Name
- Description
- OSPF Router Flags
- Administrative State

The CPAM automatically sets the ABR router flag if the router is connected to more than one area.

4

Click on the MPLS tab button.

5

Configure the Administrative State parameter.

6

Click on the RSVP tab button.

7

Configure the Administrative State parameter.

8

Click on the OK button. The Simulated Router (Create) form closes and the router appears on the topology map.

9

Click on the Impact Analysis button on the SIMULATION - IGP Model - Scenario topology map, if required.

10

Close the SIMULATION - IGP Model - Scenario topology map, if required.

END OF STEPS

19.8 To create a simulated OSPF subnet

19.8.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on the map and choose Add→OSPF Subnet from the contextual menu. The Select the OSPF Area for the new OSPF subnet form opens.

3

Perform one of the following:

a. Choose an entry and click on the OK button. The Select the OSPF Area for the new OSPF subnet form closes and the Simulated OSPF Subnet (Create) form opens.

b. Create an OSPF area. Perform the following:

1. Click on the Create OSPF Area button. The Simulated OSPF Area (Create) form opens.

2. Configure the parameters:
   - Area ID
   - Area Type
   - Name
   - Description
3. Click on the Select button next to the Color Index parameter to choose a color for the simulated network object icons and text. The Choose color form opens.

   Note:

   You can click on the Suggest button if you want the CPAM to suggest an available color.
4. Click on a color in the palette and click on the OK button. The Choose color form closes.
5. Configure the Administrative State parameter.
6. Click on the OK button. The Simulated OSPF Area (Create) form closes and the Select the OSPF Area for the new OSPF subnet form reappears.
7. Select the simulated OSPF area that you created and click on the OK button. The Select the OSPF Area for the new OSPF subnet form closes and the Simulated OSPF Subnet (Create) form opens.

4

Configure the parameters:
- IP Address
- Mask Length
- Administrative State

5

Click on the OK button. The Simulated OSPF Subnet (Create) form closes and the new simulated subnet appears on the topology map.

6

Click on the Impact Analysis button on the SIMULATION - IGP Model - Scenario topology map, if required.

7

Close the SIMULATION - IGP Model - Scenario topology map, if required.

END OF STEPS

19.9 To add a simulated OSPF link

19.9.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Perform one of the following:

a. To create a point-to-point link, select two routers by pressing the Ctrl key.

b. To create a transit network link, select one router and one subnet by pressing the Ctrl key.

3

Right-click on one of the routers or subnet and choose Add→OSPF Link. The Simulated OSPF Link (Create) form opens with the General tab displayed.

4

Click on the Select button next to the Area ID parameter. The Select OSPF Area - Simulated OSPF Link form opens.

5

Choose an entry and click on the OK button. The Select OSPF Area - Simulated OSPF Link form closes.

6

Configure the parameters:

- Unnumbered Interface
- IP Address
- Mask Length
- I/F Index
- Metric

The I/F Index is configurable only on a point-to-point link and when the Unnumbered Interface parameter is enabled. The IP Address and Mask Length parameters are configurable only when the Unnumbered Interface parameter is disabled.

7

Configure the Traffic Engineering parameter, if necessary. If you enable this parameter, additional tab buttons appear.

8

Configure the parameters:

- Name
- Description
- Administrative State

9

If you enabled the Traffic Engineering parameter, click on the Traffic Engineering tab button. Otherwise, go to Step 13 .

10

Configure the parameters:

- Maximum Bandwidth (kbps)
- Maximum Reservable Bandwidth (kbps)
- Administrative Groups
- TE Metric

11

Click on the Admin Groups tab button.

12

Select one or more administrative groups in the Unassigned column and click on the arrow icon to move them to the Assigned column.

13

Click on the RSVP tab button.

14

Configure the Administrative State parameter.

15

Click on the OK button. The Simulated OSPF Link (Create) form closes.

END OF STEPS

19.10 To add a simulated OSPF virtual link

19.10.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

To create an OSPF virtual link, select two routers by pressing the Ctrl key.

3

Right-click on one of the routers and choose Add→OSPF Virtual Link. The Simulated OSPF Virtual Link (Create) form opens with the General tab displayed.

4

Click on the Select button next to the Area ID parameter. The Select OSPF Area - Simulated OSPF Virtual Link form opens.

5

Choose an entry and click on the OK button. The Select OSPF Area - Simulated OSPF Virtual Link form closes.

Note: The list includes only area 0.0.0.0. If area 0.0.0.0 does not appear, you must create it.

6

Click on the Select button next to the Transit Area ID parameter. The Select OSPF Area form opens.

7

Specify a filter for the search, if required, and click on the Search button.

8

Choose an entry and click on the OK button. The Select OSPF Area form closes.

9

Configure the parameters:

- Name
- Description
- Administrative State

10

Click on the OK button. The Simulated OSPF Virtual Link (Create) form closes.

11

Click on the Impact Analysis button to analyze the status of the virtual links.

END OF STEPS

19.11 To create a simulated ISIS router

19.11.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on the map and choose Add→Router from the contextual menu. The Simulated Router (Create) form opens with the General tab displayed.

3

Configure the parameters:

- Router ID
- Name
- Description
- ISIS Router Flags
- Administrative State

The CPAM automatically sets the attached flag in the ISIS router flags if the router is connected to both L1 and L2 levels.

4

Click on the MPLS tab button.

5

Configure the Administrative State parameter.

6

Click on the RSVP tab button.

7

Configure the Administrative State parameter.

8

Click on the OK button. The Simulated Router (Create) form closes and the router appears on the topology map.

9

Click on the Impact Analysis button on the SIMULATION - IGP Model - Scenario topology map, if required.

10

Close the SIMULATION - IGP Model - Scenario topology map, if required.

END OF STEPS

19.12 To create a simulated ISIS subnet

19.12.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on the map and choose Add→ISIS Subnet from the contextual menu. The Select the ISIS Routing Domain for the new ISIS subnet form opens.

3

Perform one of the following:

a. Choose an entry and click on the OK button. The Select the ISIS Routing Domain for the new ISIS subnet form closes and the Simulated ISIS Subnet (Create) form opens. Go to step

b. Create a new routing domain by performing the following:

1. Click on the Create ISIS Routing Domain button. The Simulated ISIS Routing Domain (Create) form opens.
2. Configure the parameters:
   - Name
   - Description
   - Level
3. Click on the Select button next to the Color Index parameter to choose a color for the simulated network object icons and text. The Choose color form opens.

   Note:

   You can click on the Suggest button if you want the CPAM to suggest an available color.
4. Click on a color in the palette and click on the OK button. The Choose color form closes.
5. Click on the OK button to close the ISIS Routing Domain (Create) form.
6. Select the routing domain that you created and click on the OK button. The Select Routing Domain form closes and the Simulated ISIS Subnet (Create) form opens.

4

Configure the parameters:

- Pseudonode ID
- Administrative State

5

Click on the OK button. The Simulated ISIS Subnet (Create) form closes.

6

Click on the Impact Analysis button on the SIMULATION - IGP Model - Scenario topology map, if required.

7

Close the SIMULATION - IGP Model - Scenario topology map, if required.

END OF STEPS

19.13 To add a simulated ISIS link

19.13.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Perform one of the following:

a. To create a point-to-point link, select two routers by pressing the Ctrl key.

b. To create a transit network link, select one router and one subnet by pressing the Ctrl key.

3

Right-click on one of the routers or subnet and choose Add→ISIS Link. The Simulated ISIS Link (Create) form opens with the General tab displayed.

4

Click on the Select button in the Routing Domain panel. The Select Routing Domain - Simulated ISIS Link form opens.

5

Choose an entry and click on the OK button. The Select Routing Domain - Simulated ISIS Link form closes.

6

Configure the parameters:

- Unnumbered Interface
- IP Address
- Mask Length
- I/F Index
- Metric

The I/F Index is configurable only on a point-to-point link and when the Unnumbered Interface parameter is enabled. The IP Address and Mask Length parameters are configurable only when the Unnumbered Interface parameter is disabled.

7

Configure the Traffic Engineering parameter, if necessary. If you enable this parameter, additional tab buttons appear.

8

Configure the parameters:

- Name
- Description
- Administrative State

9

If you enabled the Traffic Engineering parameter, click on the Traffic Engineering tab button. Otherwise, go to Step 15 .

10

Configure the parameters:

- TE Metric
- Maximum Bandwidth (kbps)
- Maximum Reservable Bandwidth (kbps)
- Administrative Groups

11

Click on the Admin Groups tab button.

12

Select one or more administrative groups in the Unassigned column and click on the arrow icon to move them to the Assigned column.

13

Click on the RSVP tab button.

14

Configure the Administrative State parameter.

15

Click on the OK button. The Simulated ISIS Link (Create) form closes.

END OF STEPS

19.14 To view simulated IGP network data

19.14.1 General information

Perform this procedure to view configuration information about simulated network objects in a scenario. You can perform this procedure for scenarios that you created from an existing IGP administrative domain, OSPF area, checkpoint, or existing scenario.

19.14.2 Steps

1

Perform 19.4 “To create a scenario” (p. 387) to create a scenario or 19.5 “To open a scenario” (p. 392) to open an existing scenario.

2

Right-click on the SIMULATION - IGP Model - Scenario topology map and choose IGP Network Data. The SIMULATION - IGP Model - Scenario form opens.

3

Perform one of the following:

a. For an OSPF scenario, choose one of the following objects from the object drop-down menu:

- Simulated OSPF Area (CPAM: Simulated Topology)
- Simulated OSPF Link (CPAM: Simulated Topology)
- Simulated OSPF Virtual Link (CPAM: Simulated Topology)
- Simulated OSPF Subnet (CPAM: Simulated Topology)
- Simulated Router (CPAM: Simulated Topology)

Note: Alternatively, you can right-click on an object on the simulation topology map and choose Properties from the contextual menu. The properties form for the object opens with the General tab displayed.

b. For an ISIS scenario, choose one of the following from the object drop-down menu:

- Simulated ISIS Link (CPAM: Simulated Topology)
- Simulated ISIS Routing Domain (CPAM: Simulated Topology)
- Simulated ISIS Subnet (CPAM: Simulated Topology)
- Simulated Router (CPAM: Simulated Topology)

Note: Alternatively, you can right-click on an object on the simulation topology map and choose Properties from the contextual menu. The properties form for the object opens with the General tab displayed.

4

Specify a filter for the search, if required, and click on the Search button.

5

Choose an entry and click on the Properties button.

6

Perform of the following:

a. If you are viewing a simulated OSPF area, the Simulated OSPF Area (Edit) form opens with

the General tab displayed. Perform 19.15 “To view and configure a simulated OSPF area” (p. 404) .

b. If you are viewing a simulated OSPF link, the Simulated OSPF Link (Edit) form opens with the General tab displayed. Perform 19.17 “To view and configure a simulated OSPF virtual link” (p. 407) .

c. If you are viewing a simulated OSPF virtual link, the Simulated OSPF Virtual Link (Edit) form opens with the General tab displayed. Perform 19.17 “To view and configure a simulated OSPF virtual link” (p. 407) .

d. If you are viewing a simulated OSPF subnet, the Simulated OSPF Subnet (Edit) form opens with the General tab displayed. Perform 19.18 “To view and configure a simulated OSPF subnet” (p. 408) .

e. If you are viewing a simulated OSPF router, the Simulated OSPF Router (Edit) form opens with the General tab displayed. Perform 19.19 “To view and configure a simulated OSPF router” (p. 408) .

f. If you are viewing a simulated ISIS link, the Simulated ISIS Link (Edit) form opens with the General tab displayed. Perform 19.20 “To view and configure a simulated ISIS link” (p. 410) .

g. If you are viewing a simulated ISIS routing domain, the Simulated ISIS Routing Domain (Edit) form opens with the General tab displayed. Perform 19.21 “To view and configure a simulated ISIS routing domain” (p. 411) .

h. If you are viewing a simulated ISIS subnet, the Simulated ISIS Subnet (Edit) form opens with the General tab displayed. Perform 19.22 “To view and configure a simulated ISIS subnet” (p. 412) .

i. If you are viewing a simulated ISIS router, the Simulated Router (Edit) form opens with the General tab displayed. Perform 19.23 “To view and configure a simulated ISIS router” (p. 413) .

7

Close the SIMULATION - IGP Model - Scenario form, if required.

8

Close the SIMULATION - IGP Model - Scenario topology map, if required.

END OF STEPS

19.15 To view and configure a simulated OSPF area

19.15.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a scenario.

2

Right-click on the topology map and choose IGP Network Data from the contextual menu. The SIMULATION - IGP Model - Scenario form opens.

3

Choose Simulated OSPF Area (topologysim) from the object drop-down menu.

4

Specify a filter for the search, if required, and click on the Search button.

5

Choose an entry and click on the Properties button. The Simulated OSPF Area (Edit) form opens with the General tab displayed.

6

Configure the parameters:

- Name
- Area Type
- Description
- Administrative State

7

Click on the Select button next to the Color Index parameter to choose a color for the simulated network object icons and text. The Choose color form opens.

Note: You can click on the Suggest button if you want the CPAM to suggest an available color.

8

Click on a color in the palette and click on the OK button. The Choose color form closes.

9

Click on the OSPF Subnets tab button. A list of OSPF subnets in the simulated OSPF area appears.

10

Perform one of the following:

a. View and configure an existing simulated OSPF subnet by performing the following:

Note: Alternatively, you can right-click on the object on the simulation topology map and choose Properties from the contextual menu. The properties form for the object opens with the General tab displayed.

1. Choose an entry and click on the Properties button. The Simulated OSPF Subnet (Edit) form opens with the General tab displayed.
2. Configure the Administrative State parameter.
3. Click on the Originating Links tab button to view the simulated OSPF links.
4. Click on the OK button to save the configuration and close the Simulated OSPF Subnet (Edit) form.

b. Add a simulated OSPF subnet by performing the following:

Note: Alternatively, you can right-click on the simulation topology map where you want to add the object and choose Add from the contextual menu. The *Object* (Create) form for the object opens with the General tab displayed. See 19.8 “To create a simulated OSPF subnet” (p. 394) for information.

1. Click on the Add button. The Simulated OSPF Subnet (Create) form opens.
2. Configure the parameters:
   - IP Address
   - Mask Length
   - Administrative State
3. Click on the OK button. The Simulated OSPF Subnet (Create) form closes.

11

Click on the Router Bindings tab button to view a list of router bindings.

12

Click on the OK button. The Simulated OSPF Area (Edit) form closes.

END OF STEPS

19.16 To view and configure a simulated OSPF link

19.16.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a scenario.

2

Right-click on a link and choose Expand Group from the contextual menu, if required.

3

Right-click on a link and choose Properties from the contextual menu. The Simulated OSPF Link (Edit) form opens with the General tab displayed.

4

Configure the parameters:

- Metric
- Traffic Engineering
- Name
- Description
- Administrative State

5

If traffic engineering is enabled on the object, additional tab buttons appear. Click on the Traffic Engineering tab button. Otherwise, go to Step 7 .

6

Configure the parameters:

- TE Metric
- Maximum Bandwidth (kbps)
- Maximum Reservable Bandwidth (kbps)
- Administrative Groups

7

Click on the Admin Groups tab button.

8

Select one or more administrative groups in the Unassigned column and click on the arrow icon to move them to the Assigned column.

9

Click on the RSVP tab button.

10

Configure the Administrative State parameter.

11

Click on the OK button. The Simulated OSPF Link (Edit) form closes.

END OF STEPS

19.17 To view and configure a simulated OSPF virtual link

19.17.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a scenario.

2

Perform 19.14 “To view simulated IGP network data” (p. 402) to open the OSPF Virtual Link - SIMULATION (Edit) form.

3

Configure the parameters:

- Name
- Description
- Administrative State

4

Click on the OK button. The Simulated OSPF Virtual Link - SIMULATION (Edit) form closes.

END OF STEPS

19.18 To view and configure a simulated OSPF subnet

19.18.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a scenario.

2

Right-click on a subnet icon and choose Properties from the contextual menu. The Simulated OSPF Subnet (Edit) form opens with the General tab displayed.

3

Configure the Administrative State parameter.

4

Click on the Originating Links tab button.

5

View and configure a simulated OSPF link by performing the following:

1. Choose an entry and click on the Properties button. The Simulated OSPF Link (Edit) form opens with the General tab displayed.
2. Configure the parameters:
   - Name
   - Description
   - Administrative State
3. Click on the OK button to save the configuration and close the Simulated OSPF Link (Edit) form.

6

Click on the OK button. The Simulated OSPF Subnet (Edit) form closes.

END OF STEPS

19.19 To view and configure a simulated OSPF router

19.19.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a scenario.

2

Right-click on a router icon and choose Properties from the contextual menu. The Simulated OSPF Router (Edit) form opens with the General tab displayed.

3

Configure the parameters:

- Name
- Description
- OSPF Router Flags
- Administrative State

The CPAM automatically sets the ABR router flag if the router is connected to more than one area.

4

Click on the MPLS tab button.

5

Configure the Administrative State parameter.

6

Click on the RSVP tab button.

7

Configure the Administrative State parameter.

8

Click on the OSPF Area Bindings tab button to view a list of OSPF area bindings.

9

Click on the Originating Links tab button to view or add OSPF links. See 19.9 “To add a simulated OSPF link” (p. 395) for information about how to add an OSPF link.

10

Click on the OK button. The Simulated Router (Edit) form closes.

END OF STEPS

19.20 To view and configure a simulated ISIS link

19.20.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a scenario.

2

Right-click on a link and choose Expand Group from the contextual menu, if required.

3

Right-click on a link and choose Properties from the contextual menu. The Simulated ISIS Link (Edit) form opens with the General tab displayed.

4

Configure the parameters, as required:

- Metric
- Mask Length
- Traffic Engineering
- Name
- Description
- Administrative State

5

Click on the RSVP tab button.

6

Configure the Administrative State parameter.

7

If you enabled the Traffic Engineering parameter in Step 4 , click on the Traffic Engineering tab button. Otherwise, go to Step 9 .

8

Configure the parameters:

- TE Metric
- Maximum Bandwidth (kbps)
- Maximum Reservable Bandwidth (kbps)
- Administrative Groups

9

Select one or more administrative groups in the Unassigned column and click on the arrow icon to move them to the Assigned column.

10

Click on the OK button. The Simulated ISIS Link (Create) form closes.

END OF STEPS

19.21 To view and configure a simulated ISIS routing domain

19.21.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a scenario.

2

Right-click on the topology map and choose IGP Network Data from the contextual menu. The SIMULATION - IGP Model - Scenario form opens.

3

Choose Simulated ISIS Routing Domain (topologysim) from the object drop-down menu.

4

Specify a filter for the search, if required, and click on the Search button.

5

Choose an entry and click on the Properties button. The Simulated ISIS Routing Domain (Edit) form opens with the General tab displayed.

6

Configure the parameters:

- Name
- Description
- Administrative State

7

Click on the Select button next to the Color Index parameter to choose a color for the simulated network object icons and text. The Choose color form opens.

Note: You can click on the Suggest button if you want the CPAM to suggest an available color.

8

Click on a color in the palette and click on the OK button. The Choose color form closes.

9

Click on the ISIS Subnets tab button.

10

Click on the Add button to add a subnet, if required. The Simulated ISIS Subnet (Create) form opens.

Note: Alternatively, you can right-click on the simulation topology map where you want to add the object and choose Add from the contextual menu. The *Object* (Create) form for the object opens with the General tab displayed. See 19.12 “To create a simulated ISIS subnet” (p. 399) for information.

11

Configure the parameters:

- Pseudonode ID
- Administrative State

12

Click on the OK button. The Simulated ISIS Subnet (Create) form closes.

13

Click on the OK button. The Simulated ISIS Routing Domain (Edit) form closes.

END OF STEPS

19.22 To view and configure a simulated ISIS subnet

19.22.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a scenario.

2

Right-click on a subnet icon and choose Properties from the contextual menu. The Simulated ISIS Subnet (Edit) form opens with the General tab displayed.

3

Configure the Administrative State parameter.

4

Click on the OK button. The Simulated ISIS Subnet (Edit) form closes.

END OF STEPS

19.23 To view and configure a simulated ISIS router

19.23.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a scenario.

2

Right-click on a router and choose Properties from the contextual menu. The Simulated ISIS Router (Edit) form opens with the General tab displayed.

3

Configure the parameters:

- Name
- Description
- ISIS Router Flags
- Administrative State

The CPAM automatically sets the attached flag in the ISIS router flags if the router is connected to both L1 and L2 levels.

4

Click on the MPLS tab button.

5

Configure the Administrative State parameter.

6

Click on the RSVP tab button.

7

Configure the Administrative State parameter.

8

Click on the OK button to save the configuration and close the Simulated Router (Create) form.

9

Perform 19.13 “To add a simulated ISIS link” (p. 401) to create a link between two ISIS routers, if required.

10

Click on the Impact Analysis button on the SIMULATION - IGP Model - Scenario topology map.

11

Close the SIMULATION - IGP Model - Scenario topology map.

END OF STEPS

19.24 To change the administrative state of a simulated network object

19.24.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on one or more objects on the topology map, such as a link, router, or subnet, and choose Properties from the contextual menu. The Simulated *object* (Edit) form opens with the General tab displayed.

3

Set the Administrative State to Down.

4

Click on the Apply button. A confirmation window opens.

5

Click on the Yes button.

6

Click on the Impact Analysis button on the simulation topology map to view the impact on the simulated network.

7

You can bring the object administratively up by setting the Administrative State parameter on the General tab of the Simulated *object* (Edit) form to Up.

8

Click on the Apply button.

9

Click on the Impact Analysis button on the simulation topology map to view the impact on the simulated network.

10

Close the Simulated *object* (Edit) form.

END OF STEPS

19.25 To create a simulated provisioned MPLS path

19.25.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on the map and choose MPLS Model from the contextual menu. The SIMULATION-MPLS Model form opens.

Note: Alternatively, you can press the Ctrl key and select two or more routers. Right-click on one of the routers and choose Add→LSP. The Provisioned MPLS Path, MPLS-SIMULATION (Create) form opens with the General tab displayed.

The Source System IP parameter is automatically configured with the first router you select. The remaining routers are inserted as hops, as described in Step 8 .

3

Click on the Create button and choose Create LSP. The Provisioned MPLS Path, MPLS-SIMULATION (Create) form opens with the General tab displayed.

4

Click on the Select button next to the Source System IP parameter. The Select Source System IP / Router - IGP- SIMULATION form opens.

5

Specify a filter for the search, if required, and click on the Search button. A list of routers appears.

6

Choose an entry and click on the OK button. The Select Source System IP / Router - IGP-SIMULATION form closes.

7

Configure the parameters:

- Name
- Description
- Administrative State

8

Click on the Hops tab button.

9

Click on the Insert Hop button. The Provisioned Hop, MPLS - SIMULATION (Create) form opens.

10

Click on the Select button next to the IP Address parameter. The Select Hop IP Address form opens.

11

Specify a filter for the search, if required, and click on the Search button.

12

Choose an entry and click on the OK button. The Select Hop IP Address form closes.

13

Configure the Hop Type parameter.

14

Click on the OK button. The Provisioned Hop, MPLS - SIMULATION (Create) form closes. A dialog box appears.

15

Click on the OK button. The dialog box closes.

16

Repeat Step 9 to Step 15 to add additional hops.

17

Click on the OK button. The Provisioned MPLS Path, MPLS-SIMULATION (Create) form closes.

18

Close the SIMULATION-MPLS Model form.

19

Close the SIMULATION - *Protocol* Model - Scenario topology map.

END OF STEPS

19.26 To create a simulated LSP

19.26.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on the map and choose MPLS Model from the contextual menu. The SIMULATION-MPLS Model form opens.

Note: Alternatively, you can press the Ctrl key and select two routers. Right-click on one of the routers and choose Add→LSP. The Simulated LSP, MPLS-SIMULATION (Create) form opens with the General tab displayed.
The Source System IP and Source IP Address parameters are automatically configured with the first router that you select. The Destination System IP and Destination IP Address parameters are automatically configured with the second router that you select.

3

Click on the Create button and choose Create LSP. The Simulated LSP, MPLS-SIMULATION (Create) form opens with the General tab displayed.

4

Configure the parameters:

- Name
- Description
- Processing Order

5

Configure the source.

1. Click on the Select button next to the Source System IP parameter. The Select Source System IP / Router - IGP- SIMULATION form opens.
2. Specify a filter for the search, if required, and click on the Search button. A list of routers appears.
3. Choose an entry and click on the OK button. The Select Source System IP / Router - IGP-SIMULATION form closes.
4. Click on the Select button next to the Source IP Address parameter. The Select Source IP Address - IGP- SIMULATION form opens.
5. Specify a filter for the search, if required, and click on the Search button. A list of routers appears.
6. Choose an entry and click on the OK button. The Select Source IP Address - IGP-SIMULATION form closes.

6

Configure the destination.

1. Click on the Select button next to the Destination System IP parameter. The Select Destination System IP / Router - IGP- SIMULATION form opens.
2. Specify a filter for the search, if required, and click on the Search button. A list of routers appears.
3. Choose an entry and click on the OK button. The Select Destination System IP / Router - IGP- SIMULATION form closes.
4. Click on the Select button next to the Destination IP Address parameter. The Select Destination IP Address - IGP- SIMULATION form opens.
5. Specify a filter for the search, if required, and click on the Search button. A list of routers appears.
6. Choose an entry and click on the OK button. The Select Destination IP Address - IGP-SIMULATION form closes.

7

Configure the Administrative State parameter.

8

Click on the Properties tab button.

9

Configure the parameters:

- Enable CSPF
- Enable TE Metric
- Reserved Bandwidth
- Hop Limit
- ECMP Tie Breaker
- Measured Bandwidth

The Measured Bandwidth parameter is auto-populated when your scenario uses imported LSPs that are enabled for statistics collection.

10

Click on the Administrative Groups tab button.

11

Choose one or more administrative groups from the Unassigned list in the Included Groups panel and click on the right arrow button. The administrative group or groups move to the Assigned list.

Note: The links in the calculated CSPF must include the specified administrative groups.

12

Choose one or more administrative groups from the Unassigned list in the Excluded Groups panel and click on the right arrow button. The administrative group or groups move to the Assigned list.

Note: The links in the calculated CSPF must exclude the specified administrative groups.

13

Create one or more LSP paths.

1. Click on the LSP Paths tab button.
2. Click on the Create LSP Path button. The Simulated LSP Path SIMULATION (Create) form opens with the General tab displayed.
3. Configure the parameters:
   - Name
   - Description
   - Type
   - Standby

   The Standby parameter is configurable when the Type parameter is set to secondary.

4. Click on the Select button next to the Path ID parameter. The Select Provisioned MPLS Path - Simulated LSP Path - MPLS - SIMULATION form opens with a list of provisioned paths.
5. Choose an entry and click on the OK button. The Select Provisioned MPLS Path - Simulated LSP Path - MPLS - SIMULATION form closes.
6. Configure the Administrative State parameter.
7. Click on the Properties tab button.
8. Configure the parameters:
   - Reserved Bandwidth
   - Hop Limit
   - Admin Groups Included
   - Admin Groups Excluded
   - ECMP Tie Breaker

   You can specify that the parameter value is inherited from the LSP configuration using the Inherit Value parameter.
9. Click on the Administrative Groups tab button.
10. Choose one or more administrative groups from the Unassigned list in the Included Groups panel and click on the right arrow button. The administrative group or groups move to the Assigned list.

    Note:

    The links in the calculated CSPF must include the specified administrative groups.
11. Choose one or more administrative groups from the Unassigned list in the Excluded Groups panel and click on the right arrow button. The administrative group or groups move to the Assigned list.

    Note:

    The links in the calculated CSPF must exclude the specified administrative groups.
12. Click on the following tab buttons to view information.
    - Provisioned Path
    - Actual Path—the actual path is available only after the impact analysis if the LSP path is operationally up.
13. Click on the Apply button.
14. Click on the Path Records tab button.
15. Click on the Search button. A list of LSP path records appears.
16. Choose an entry and click on the Properties button. The LSP Path Record SIMULATION (Edit) form opens with the General tab displayed.
17. Click on the following tab buttons to view information.
    - Scenario
    - Segments
18. Close the LSP Path Record SIMULATION (Edit) form.

14

Click on the OK button. The Simulated LSP Path SIMULATION (Edit) form closes.

15

Click on the Impact Analysis button on the SIMULATION - *Protocol* Model - Scenario topology map to converge the topology. The Legend - SIMULATION - *Protocol* Model - Scenario form opens with the Last Impact Results tab displayed.

Note: For quick reference to the last results of the impact analysis, you can keep the Legend - SIMULATION - *Protocol* Model - Scenario form open while you are working with the simulation topology.

16

Click on the View Impact Details button, if required, to view the details of the impact analysis. The Action Event - Impact Analysis - SIMULATION - Scenario (Edit) form opens with the General tab displayed.

17

Click on the following tab buttons to view information about the impact analysis:

- Attributes
- Scenario
- IP Paths
- LSP Paths

18

Close the Action Event - Impact Analysis - SIMULATION - Scenario (Edit) form.

19

Click on the Close button to close the Legend - SIMULATION - *Protocol* Model - Scenario form.

20

Close the SIMULATION - *Protocol* Model - Scenario topology map.

END OF STEPS

19.27 To simulate the impact of LSP bandwidth changes on link utilization

19.27.1 Purpose

You can assess link utilization when you configure various bandwidth values for the LSPs on the link.

19.27.2 Steps

1

Open a scenario; see 19.5 “To open a scenario” (p. 392). An IGP topology is displayed on the map.

To create a scenario, see 19.4 “To create a scenario” (p. 387).

2

Click on the MPLS model icon and choose one or more LSPs.

3

Open the properties form for each of the selected LSPs, click on the Properties tab and configure the Measured Bandwidth parameter.

The Measured Bandwidth parameter is auto-populated when your scenario uses imported LSPs that are enabled for statistics collection. Use the auto-populated values if required.

4

Click Impact Analysis. The Legend-SIMULATION-IGP Model-Scenario form opens and displays the Last Impact Results tab. Close or move the Legend form.

5

Select the MPLS Link Utilization Colors check box. The colors on the map change to colors that correspond to link utilization values.

Link utilization is expressed as a percentage of the total capacity of the link.

Click on the Colors tab of the Legend form to see the utilization values that correspond to the colors. To open the Legends form again, click on the Legend icon.

White indicates a multi-utilization link, meaning that utilization values are different in one direction than the other.

6

To see utilization values for multi-utilization links, right-click on a white-colored link and choose Expand Group. The map shows links in both directions, each with a color that shows its utilization.

7

Select a link on the map to view the properties form for the link. The Utilization parameter displays link utilization as a percentage.

You can modify the Link Bandwidth parameter to simulate the impact of various link capacities.

8

To change measured bandwidth values for LSPs:

1. Click on the MPLS Model icon and choose Simulated LSP from the object drop-down.

2. Choose the required LSP. The Simulated LSP properties form opens.
3. Click on the Properties tab and configure the Measured bandwidth tab.

9

Click Impact Analysis to run the simulation.

You must select the MPLS Link-utilization Colors check box each time you run a new impact analysis simulation.

END OF STEPS

19.28 To import MPLS objects from the NFM-P

19.28.1 General information

Perform this procedure to import MPLS objects from the NFM-P for impact analysis simulations. You can import the following MPLS objects:

- LSPs
- LSP paths
- MPLS provisioned paths

You cannot import LDP objects from the NFM-P.

19.28.2 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on the map and choose MPLS Model from the contextual menu. The SIMULATION-MPLS Model form opens.

3

Click on the Import LSPs Config button and perform one the following:

a. Choose All Simulated LSPs from Other Scenario from the contextual menu to import all existing simulated LSPs from another scenario. The Select Scenario to import all its Simulated LSPs form opens. Go to Step 4 .

b. Choose Selected Simulated LSPs from Other Scenario from the contextual menu to select and import existing simulated LSPs from another scenario. The Import Selected Simulated LSPs from Other Scenario form opens. Go to Step 5 .

c. Choose Selected LSPs from Real Network from the contextual menu to import selected existing real LSPs from a real network. The Import Selected LSPs from Real Network form opens. Go to Step 7 .

d. Choose All LSPs from Real Network from the contextual menu to import all existing real

LSPs from a real network. A dialog box appears. Click on the Yes button and go to Step 9 .

4

Choose an entry and click on the OK button. The Select Scenario to import all its Simulated LSPs form closes. Go to Step 9 .

5

Specify a filter for the search, if required, and click on the Search button. A list of simulated LSPs appears.

6

Choose an entry and click on the OK button. The Import Selected Simulated LSPs from Other Scenario form closes. Go to Step 9 .

7

Specify a filter for the search, if required, and click on the Search button. A list of dynamic LSPs appears.

8

Choose an entry and click on the OK button. The Import Selected LSPs from Real Network form closes.

9

Close the SIMULATION-MPLS Model form.

10

Click on the Impact Analysis button on the SIMULATION - *Protocol* Model - Scenario topology map to run the analysis. When the impact analysis is complete, Topology Converged is displayed, and the Legend - SIMULATION - *Protocol* Model - Scenario form opens with the Last Impact Results tab displayed.

Note: For quick reference to the last results of the impact analysis, you can keep the Legend - SIMULATION - *Protocol* Model - Scenario form open while you are working with the simulation topology.

11

Click on the View Impact Details button, if required, to view the details of the impact analysis. The Action Event - Impact Analysis - SIMULATION - Scenario (Edit) form opens with the General tab displayed.

12

Click on the following tabs to view information about the impact analysis:

- Attributes

- Scenario
- IP Paths
- LSP Paths
- Services

13

Close the Action Event - Impact Analysis - SIMULATION - Scenario (Edit) form.

14

Click on the Close button to close the Legend - SIMULATION - *Protocol* Model - Scenario form.

15

Close the SIMULATION - *Protocol* Model - Scenario topology map.

END OF STEPS

19.29 To import IP paths

19.29.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on the topology map and choose Simulated Path Monitoring from the contextual menu. The Simulated Path Monitoring form opens.

3

Click on the Import Paths button and choose one of the following:

a. All Simulated Paths from Other Scenario—import all of the simulated IP paths from an existing scenario. The All Simulated Paths from Other Scenario form opens. Go to Step 4 .

b. Selected Simulated Paths from Other Scenario—import selected simulated IP paths from an existing scenario. The Import Selected Simulated Paths from Other Scenario form opens. Go to Step 5 .

c. Selected Paths from Real Network—import selected real IP paths from a real network. The Import Selected Paths from Real Network form opens. Go to Step 6 .

4

Perform the following:

1. Choose an entry and click on the OK button. The All Simulated Paths from Other Scenario form closes.
2. Go to Step 7 .

5

Perform the following:

1. Specify a filter for the search, if required and click on the Search button.
2. Choose an entry and click on the OK button. The Import Selected Simulated Paths from Other Scenario form closes.
3. Go to Step 7 .

6

Perform the following:

1. Specify a filter for the search, if required and click on the Search button.
2. Choose an entry and click on the OK button. The Import Selected Paths from Real Network form closes.

7

Close the Simulated Path Monitoring form.

END OF STEPS

19.30 To view historical LSP path records

19.30.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on the map and choose MPLS Model from the contextual menu. The SIMULATION-MPLS Model form opens.

3

Choose Simulated LSP (CPAM:Simulated Topology) from the object drop-down menu.

4

Specify a filter for the search, if required, and click on the Search button. A list of simulated LSPs appears.

5

Choose an entry and click on the Properties button. The Simulated LSP - SIMULATION (Edit) form opens with the General tab displayed.

6

Click on the Path Records tab button.

7

Specify a filter for the search, if required, and click on the Search button. A list of LSP path records appears.

8

Choose an entry and perform one of the following:

a. Click on the Properties button. The LSP Path Record - SIMULATION (Edit) form opens with the General tab displayed. Go to Step 9 .

b. Click on the Navigate button and choose Historical LSP Path from the contextual menu. The appropriate path is highlighted on the topology map. Go to Step 15 .

9

View the following information.

- record timestamp
- error code
- error details
- LSP details

10

Click on the Segments path button.

11

Choose an entry and click on the Properties button. The LSP Path Segment - SIMULATION (Edit) form opens with the General tab displayed.

12

View the following information.

- segment type
- link type
- protocol
- segment start and end system and egress/ingress IP addresses, and router IDs
- LSP details
- protocol details

13

Close the LSP Path Segment - SIMULATION (Edit) form.

14

Close the LSP Path Record - SIMULATION (Edit) form

15

Close the Simulated LSP - SIMULATION (Edit) form.

16

Close the SIMULATION-MPLS Model form.

END OF STEPS

19.31 To perform a manual resignal of an LSP

19.31.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on the map and choose MPLS Model from the contextual menu. The SIMULATION-MPLS Model form opens.

3

Choose Simulated LSP (CPAM:Simulated Topology) from the object drop-down menu.

4

Specify a filter for the search, if required, and click on the Search button. A list of simulated LSPs appears.

5

Choose an entry and click on the Properties button. The Simulated LSP - SIMULATION (Edit) form opens with the General tab displayed.

6

Click on the Trigger Resignal button.

7

Specify a filter for the search, if required, and click on the Search button. A list of LSP path records appears.

8

Choose an entry and click on the Properties button. The LSP Path Record - SIMULATION (Edit) form opens with the General tab displayed.

9

View the following information.

- record timestamp
- error code
- error details
- LSP details

10

Click on the Segments path button.

11

Choose an entry and click on the Properties button. The LSP Path Segment - SIMULATION (Edit) form opens with the General tab displayed.

12

View the following information.

- segment type
- link type
- protocol
- segment start and end system and egress/ingress IP addresses, and router IDs
- LSP details
- protocol details

13

Close the LSP Path Segment - SIMULATION (Edit) form.

14

Close the LSP Path Record - SIMULATION (Edit) form

15

Close the Simulated LSP - SIMULATION (Edit) form.

16

Close the SIMULATION-MPLS Model form.

END OF STEPS

19.32 To capture the path of LSP paths associated with an LSP

19.32.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on the map and choose MPLS Model from the contextual menu. The SIMULATION-MPLS Model form opens.

3

Choose Simulated LSP (CPAM:Simulated Topology) from the object drop-down menu.

4

Specify a filter for the search, if required, and click on the Search button. A list of simulated LSPs appears.

5

Choose an entry and click on the Properties button. The Simulated LSP - SIMULATION (Edit) form opens with the General tab displayed.

6

Click on the Path Records tab button.

7

Click on the Capture Paths button. A new LSP path record appears in the list.

8

Close the Simulated LSP - SIMULATION (Edit) form.

END OF STEPS

19.33 To monitor a simulated IP path

19.33.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on the topology map and choose Simulated Path Monitoring from the contextual menu. The Simulated Path Monitoring form opens.

3

Click on the Create button. The Simulated IP Path Monitor (Create) form opens with the General tab displayed.

Note: Alternatively, you can press the Ctrl key and select two routers. Right-click on one of the routers and choose Add→IP Path Monitor. The Simulated IP Path Monitor (Create) form opens with the General tab displayed.

4

Configure the parameters:

- Name
- Description
- Monitor State

5

Configure the Source IP parameter or use the Select button to choose a source router.

6

Configure the Source Length parameter.

7

Configure the Destination IP parameter or use the Select button to choose a destination router.

8

Configure the Destination Length parameter.

9

Click on the Apply button to save the configuration.

10

Click on the Path History tab button to view monitored IP paths.

11

Close the Simulated IP Path Monitor (Create) form.

12

Close the Simulated Path Monitoring form.

END OF STEPS

19.34 To delete a simulated network object

19.34.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on one or more objects on the topology map, such as a link, router, or subnet, and choose Delete from the contextual menu. A confirmation window appears.

3

Enable the I understand the implications of this action checkbox and click on the Yes button. The confirmation window closes and the object is deleted.

4

Click on the Impact Analysis button. The impact of the object deletion is displayed on the topology map.

Note: Nokia recommends that you do not delete routers and links from the simulation topology as this may cause an incomplete highlight of historical paths. Nokia recommends that you administratively shut down these objects, as described in 19.24 “To change the administrative state of a simulated network object” (p. 414) .

END OF STEPS

19.35 To highlight a simulated LSP

19.35.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on the map and choose MPLS Model from the contextual menu. The SIMULATION-MPLS Model form opens.

3

Choose Simulated LSP (CPAM:Simulated Topology) from the object drop-down menu.

4

Specify a filter for the search, if required, and click on the Search button. A list of simulated LSPs appears.

5

Choose an entry and click on the Properties button. The Simulated LSP - SIMULATION (Edit) form opens with the General tab displayed.

6

Click on the Navigate button. Choose one of the following from the contextual menu:

- Provisioned Path for the Active Path

- Operational Paths
- Active Path
- Provisioned Path

The appropriate path is highlighted on the topology map.

7

Close the Simulated LSP - SIMULATION (Edit) form.

8

Close the SIMULATION-MPLS Model form.

END OF STEPS

19.36 To highlight a simulated historical LSP path record

19.36.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on the map and choose MPLS Model from the contextual menu. The SIMULATION-MPLS Model form opens.

3

Choose Simulated LSP (CPAM:Simulated Topology) from the object drop-down menu.

4

Specify a filter for the search, if required, and click on the Search button. A list of simulated LSPs appears.

5

Choose an entry and click on the Properties button. The Simulated LSP - SIMULATION (Edit) form opens with the General tab displayed.

6

Click on the Path Records tab button.

7

Choose an entry and click on the Navigate button on the right side of the form.

8

Choose Historical LSP Path from the contextual menu. The appropriate path is highlighted on the topology map.

9

Close the Simulated LSP - SIMULATION (Edit) form.

10

Close the SIMULATION-MPLS Model form.

END OF STEPS

19.37 To highlight a simulated LSP path

19.37.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on the map and choose MPLS Model from the contextual menu. The SIMULATION-MPLS Model form opens.

3

Choose Simulated LSP (CPAM:Simulated Topology) from the object drop-down menu.

4

Specify a filter for the search, if required, and click on the Search button. A list of simulated LSPs appears.

5

Choose an entry and click on the Properties button. The Simulated LSP - SIMULATION (Edit) form opens with the General tab displayed.

6

Click on the LSP Paths tab button.

7

Choose an LSP path and click on the Navigate button on the right side of the form. Choose one of the following from the contextual menu:

- Provisioned LSP Path
- Actual LSP Path

The appropriate path is highlighted on the topology map.

8

Close the Simulated LSP - SIMULATION (Edit) form.

9

Close the SIMULATION-MPLS Model form.

END OF STEPS

19.38 To highlight SPF links

19.38.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

Note: You can only create an SPF highlight request if the topology is converged. The grey operational mode indicator at the top-left of the topology map must be Topology converged. If the operational indicator is yellow, click on the Impact Analysis button. The Legend - SIMULATION - IGP Model - Scenario form opens with the Last Impact Results tab displayed. Click on the Close button.

2

Right-click on the map and choose Highlight→Paths→IP→SPF from the contextual menu. The Find Object form opens.

3

Configure the First IP parameter or use the Select button to select a router if the source IP address is a router.

4

Configure the Second IP parameter or use the Select button to select a router if the destination IP address is a router.

Note: Alternatively, you can press the Ctrl key and click on a source and destination router or link, right-click and choose Highlight IGP Links→Highlight SPF from the contextual menu. The First IP and Second IP parameters are configured with the IP address of the selected routers.

5

Click on the OK button. The Find Object form closes and the SPF is highlighted on the simulation topology map.

6

To remove the SPF highlight, click on the Legend button and choose Highlight Sessions from the contextual menu. The Legend - SIMULATION - IGP Model form opens with the Highlight Sessions tab displayed

7

Disable the checkboxes of the highlights you want to remove from the topology map. You can click on the Clear All button to disable all of the checkboxes.

8

Click on the Apply button. The selected highlights are removed from the topology map.

9

Click on the Close button. The Legend - SIMULATION - IGP Model form closes.

END OF STEPS

19.39 To highlight CSPF

19.39.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

Note: You can only create a CSPF highlight request if the topology is converged. The grey operational mode indicator at the top-left of the topology map must be Topology converged. If the operational indicator is yellow, click on the Impact Analysis button. The Legend - SIMULATION - IGP Model - Scenario form opens with the Last Impact Results tab displayed. Click on the Close button.

2

Perform one of the following:

a. Right-click on the map and choose Highlight IGP Links→Highlight from the contextual menu. The Highlight CSPF Request form opens with the General tab displayed.

b. Perform the following:

1. Press the Ctrl key and click on a source and destination router or link.
2. Right-click on a router and choose Highlight CSPF from the contextual menu. The Highlight CSPF Request form opens with the General tab displayed.

3

Configure the parameters:

- Protocol
- Required Bandwidth
- Hop Limit

- System Instance ID

4

Click on the Select button next to the Source IP parameter. The Select Source Router form opens.

Note: If you performed Step 2 b , the Source IP parameter is already configured with the source router IP address.

5

Specify a filter and click on the Search button. A list of simulated routers appears.

6

Choose an entry and click on the OK button. The Select Source Router form closes and the Highlight CSPF Request form reappears with the source router information.

7

Click on the Select button next to the Destination FEC parameter. The Select Destination FEC form opens.

Note: If you performed Step 2 b , the Destination FEC parameter is already configured with the destination router IP address.

8

Specify a filter and click on the Search button. A list of simulated routers appears.

9

Choose an entry and click on the OK button. The Select Destination FEC form closes and the Highlight CSPF Request form reappears with the destination information.

10

Click on the Admin Groups tab button.

11

Choose an administrative group from the Unassigned list in the Included Groups panel and click on the right arrow button. The administrative group moves to the Assigned list.

Note: The links in the calculated CSPF must include the specified administrative groups.

12

Choose an administrative group from the Unassigned list in the Excluded Groups panel and click on the right arrow button. The administrative group moves to the Assigned list.

Note: The links in the calculated CSPF must exclude the specified administrative groups.

13

Click on the Excluded Routers tab button.

14

Specify the routers that are to be excluded from the CSPF highlight. The highlighted CSPF must not pass through the routers with the specified router IDs. Perform the following:

1. Click on the Add button. The Select Excluded Routers form opens.
2. Specify a filter and click on the Search button. A list of simulated routers appears.
3. Choose one or more routers and click on the OK button. The Select Excluded Routers form closes.

15

Click on the Excluded Egress IP Addresses tab button.

16

Specify the egress IP addresses that are to be excluded from the CSPF highlight. The highlighted CSPF must not pass through the egress interfaces with the specified IP addresses.

1. Click on the Add button. The Select Excluded Egress IP Links form opens.
2. Select an icon from the top-left panel.
3. Specify a filter and click on the Search button.
4. Choose one or more links and click on the OK button. The Select Excluded Egress IP Links form closes.

17

Click on the OK button. The Highlight CSPF Request form closes and the CSPF is highlighted on the topology map.

18

To remove the CSPF highlight, click on the Legend button and choose Highlight Sessions from the contextual menu. The Legend - SIMULATION - IGP Model form opens with the Highlight Sessions tab displayed

19

Disable the checkboxes of the highlights you want to remove from the topology map. You can click on the Clear All button to disable all of the checkboxes.

20

Click on the Apply button. The selected highlights are removed from the topology map.

21

Click on the Close button. The Legend - SIMULATION - IGP Model form closes.

END OF STEPS

19.40 To highlight a historical simulated IP path record

19.40.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on the topology map and choose Simulated Path Monitoring from the contextual menu. The Simulated Path Monitoring form opens.

3

Specify a filter for the search, if required and click on the Search button.

4

Choose an entry and click on the Properties button. The Simulated IP Path Monitor (Edit) form opens with the General tab displayed.

5

Click on the Path History tab button.

6

Choose an entry and click on the Navigate button. The SIMULATION - IGP Model - Scenario map opens with the highlighted path.

7

Close the Simulated IP Path Monitor (Edit) form.

8

Close the Simulated Path Monitoring form.

END OF STEPS

19.41 To view the history of simulation events

19.41.1 Steps

1

Perform 19.5 “To open a scenario” (p. 392) to open a simulation topology map.

2

Right-click on the topology map and choose Change History from the contextual menu.

3

The SIMULATION - Change History - Scenario form opens.

4

Specify a filter for the search, if required, and click on the Search button.

5

Choose an entry and click on the Properties button. The *Action/Change* Event (Edit) form opens with the General tab displayed.

6

View information about the event, such as:

- the time the event occurred
- the type of event (action or change)
- a description of the event
- the change action
- the user that triggered the event

7

Click on the Changed Attributes tab button. A list of attributes to which changes were made is displayed.

8

Close the *Action/Change* Event (Edit) form.

9

Close the SIMULATION - Change History - Scenario form.

END OF STEPS

19.42 To manage impact analysis sessions

19.42.1 General information

Perform this procedure to view and manage impact analysis sessions. You need the appropriate scope of command role to perform this procedure.

19.42.2 Steps

1

Choose Tools→Route Analysis→Simulated Impact Analysis from the NFM-P main menu. The Simulated Impact Analysis form opens.

2

Click on Session (simulator) in the top-left panel.

3

Specify a filter for the search, if required, and click on the Search button. A list of sessions appears.

4

To view a session, select the entry and click on the Properties button. The Session (Edit) form opens with the General tab displayed with the following session details:

- session ID
- start time
- user name

5

Click on the Properties button in the Scenario panel to view the scenario configuration. The Scenario - *scenario_name* (Edit) form opens with the General tab displayed.

6

Close the Scenario - *scenario_name* (Edit) form.

7

To delete a session, select the entry and click on the Delete button. A confirmation window opens.

8

Click on the Yes button. A dialog window opens.

9

Click on the OK button. A warning window opens.

10

Click on the OK button.

11

Close the Simulated Impact Analysis form.

END OF STEPS

Part VIII: XML API

Overview

Purpose

This volume provides XML API information.

Contents

20 XML API

20.1 XML API overview

20.1.1 Introduction

OSS clients access CPAM-related objects and operations using the XML API interface. The XML API interface consists of XML and SOAP over HTTP, and XML over JMS messaging.

20.2 XML API objects and configurations overview

20.2.1 Introduction

The following sections describe the objects that can be accessed using the XML API and the configurations that can be performed.

20.2.2 CPAA manual switchover

The XML API can be used to manually switchover from a failed CPAA to the redundant CPAA. A switchover can only be performed once every ten minutes. A warning will be sent to the XML API if another switchover is requested prior to this.

20.2.3 Route analyzer

All CPAA configurations can be performed through the XML API, including the use of the XML API to configure and monitor protocol and device configurations such as OSPF and ISIS. The JMS interface notifies the XML API of any changes to the CPAA.

20.2.4 Topology model

The XML API provides a read-only interface for topology objects, such as areas, routers, links, networks, and baselines. The JMS interface notifies the XML API of any changes to the topology model, including baselines.

20.2.5 Topology operations

The following topology operations can be performed through the XML API:

- **checkpoint**
  Includes setting, removing, and resetting the baseline for the OSPF. The JMS interface notifies the NFM-P of the objects affected by the baseline operation.
- **route calculations**
  See 4.3 “OSPF topology overview” (p. 49) for information about shortest path calculations.

20.2.6 Path and monitored prefix

BGP monitored prefix

The following operations can be performed through XML API:

- creation and deletion of monitors
- retrieval of BGP monitored prefix data

Part IX: Appendix

Overview

Purpose

This volume contains an appendix that provides information about CPAM MIB support for GNEs, and RFCs related to MIB support.

Contents

A CPAM MIB support for GNEs

A.1 CPAM MIB support for GNEs

A.1.1 Overview

The CPAM supports the limited management of GNEs. The CPAM support of GNEs requires the proper MIB support on GNEs.

The NFM-P mediation engine supports standard MPLS MIBs. The GNEs managed by the NFM-P using standard MIBs must use attributes, IDs and traps in a specific manner to ensure proper operation. Otherwise, LSP objects may be represented incorrectly in the NFM-P. Consider the following regarding GNE standard MIB implementation of MPLS paths.

The NFM-P defines an LSP as an end-to-end path between source and destination label-switched routers. An MPLS path is created when a new mplsTunnel in the mplsTunnelTable is created (a new mpls.Tunnel object announced by a mplsTunnelUp trap). An LSP is also created with an LSP ID corresponding to the mplsTunnelIndex, unless one already exists due to the existence of multiple paths under one LSP.

A route associated with an LSP can be an actual path or a configured path. There can be only one actual path. A configured path contains a primary path, and may also contain multiple secondary and standby paths. The NFM-P groups all of the paths related to an LSP to manage them as a related entity. The GNE must use the same mplsTunnelIndex attribute for a set of primary and standby paths.

The standard MIB does not differentiate between secondary and standby paths, but it does differentiate between primary and secondary paths. The mplsTunnelPrimaryInstance attribute distinguishes the primary from the standby and secondary paths within the LSP. For example, an LSP has three paths (instance 1,2, and 3 respectively) using the same mplsTunnelIndex. Instance 1 is the primary path. The mplsTunnelPrimaryInstance attribute of instance 1 must be set to 0. The mplsTunnelPrimaryInstance attribute is set to 1 for tunnel instances 2 and 3.

The NFM-P relies on the RSVP sessions to determine the hops of the primary and standby paths. Hops are read from the mplsTunnelHopTable and the mplsTunnelARHopTable.

The bit-field attribute “mplsTunnelSessionAttributes” determines whether fast reroute is available. Fast reroute is bit 0. The attribute should be set to 1 or an odd number to identify that the LSP is using fast reroute. Detour or bypass hop records are not supported, because the standard MIB does not provide enough information to associate an RSVP session with a detour of bypass.

The NFM-P triggers a resync of the path when it receives the following traps from the NE:

- **The “mplsTunnelRerouted” trap when a path hop changes.**
  No “mplsTunnelDown” trap or object deletion should occur.
- **The “mplsTunnelReoptimized” when the path is re-optimized.**
  No “mplsTunnelDown” trap or object deletion should occur.
- **The “mplsTunnelDown” when a path is down.**

A path is configured but the source cannot find a path or cannot successfully signal the path. After a the NFM-P performs the resync, the tunnel should still exist in the tunnel table of the GNE. The path status in the NFM-P is set to Down.

- **The “mplsTunnelUp” trap when the path status is Up.**
  The path can be successfully signaled. After the NFM-P performs the resync, the tunnel should still exist in the tunnel table of the GNE. The path status in the NFM-P is set to Up.
- **The “mplsTunnelDown” trap when the user deletes a path.**
  After the NFM-P performs the resync, the tunnel should no longer exist in the tunnel table of the GNE. The path is deleted in the NFM-P and the LSP is deleted if no other path is related to this LSP (no more paths with the same mplsTunnelIndex).

Note: Standard MIBs support read-only mode for the path objects. LSPs or paths can not be configured from the NFM-P.

See “To prepare a GNE for NFM-P management” in the *NSP NFM-P Classic Management User Guide* for information about how to add a routing MIB to a GNE profile.

A.2 RFCs

A.2.1 Purpose

The following section lists the RFCs that provide standard MIB support in the CPAM.

A.2.2 BGP Standard MIB

RFC 1657 BGP-STD (Read-only)

A.2.3 IGMP

RFC 2933 IGMP-STD (Read-only)

A.2.4 ISIS Experimental MIB

ISIS-STD MIB (Read-only)

A.2.5 ISIS Standard MIB

RFC 4444 ISIS-STD MIB (Read-only)

A.2.6 MPLS LDP Standard MIB

RFC 3815 MPLS-LDP-STD MIB (Read-only)

A.2.7 MPLS Label Switching Router

RFC 3813 MPLS-LSR-STD MIB (Read-only)

A.2.8 MPLS Traffic Engineering MIB

RFC 3812 MPLS-TE-STD MIB (Read-only)

A.2.9 OSPF Standard MIB

RFC 1850 OSPFV2-STD MIB (Read-only)

A.2.10 PIM

RFC 5060 PIM-STD MIB (Read-only)

A.2.11 PIM Experimental

PIM-EXP MIB (Read-only)

A.2.12 RSVP Standard MIB

RFC 2206 RSVP-STD MIB (Read-only)

CPAM supports RSVP interfaces, but not RSVP sessions because of the minimal information supported by the standard.