NOKIA

NSP
Network Services Platform
Release 22.11

Network Supervision Application Help

3HE-18136-AAAE-TQZZA

Issue 1

November 2022

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 *Network Supervision Application Help* introduces the Network Supervision application GUI to operators and administrators by describing application usage and features.

Scope

The help for Network Supervision covers the full set of application features; however, some feature sets described in the help require the purchase and configuration of additional feature packages.

See the *NSP System Architecture Guide* for more information about feature packages and installation options.

Network Supervision functions are available for OSS using programmable APIs. For general information about developer support, see the API documentation page on the Network Developer Portal.

For specific documentation about REST APIs for Network Supervision, click on API Reference in the Network Supervision row.

Document support

Customer documentation and product support URLs:

- Documentation Center
- Technical support

How to comment

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

1 Network Supervision

1.1 What is Network Supervision?

The Network Supervision application is a browser-based tool for monitoring the health of network equipment. It allows you to identify, investigate, and resolve problems with objects such as routers, cards, ports, physical links, and virtual network functions.

Network Supervision provides high-level visibility of equipment problems in the network, and allows quick navigation to specific objects for closer inspection and analysis. It also provides visualization tools and task flows for troubleshooting, to determine the root causes and impacts of equipment issues. A variety of display formats allows you to view and manage large amounts of information according to your needs and methods.

Network Supervision provides flexible task flows; there are multiple ways to identify and investigate problems. For example, you may decide to investigate issues based on active monitoring, Analytics reports, customer tickets, or historical problems. You can monitor and investigate links as well as NEs.

Network Supervision also allows you to monitor virtualized network functions (VNFs), such as load balancers, firewalls, and NAT, in a virtualized or datacenter environment where network functions are uncoupled from the underlying hardware. VNF management is provided by the external application CBAM, using access points available to Network Supervision. VNF threshold policies and policy templates are also supported.

1.2 What are views and supervision groups?

In the Network Supervision application, equipment is organized into **supervision groups**, which are then added to a **view** that allows you to monitor the health of large amounts of equipment in a single display.

A supervision group is made up of NEs that are grouped according to some logical principle, for example, by region, equipment type, or customer.. A view provides an even high-level overview of the supervision groups that belong to the view. Using visual KPIs, operators can identify problems at the view and supervision group levels, then drill down to investigate specific objects.

Views and supervision groups are created and managed by an administrator using the Group Manager application.

1.3 How do I change the view?

Views are created and managed by an administrator using the Group Manager application. When you select a view, it remains the default view for subsequent sessions, until it is changed.

1

In the Network Supervision application, click **More** ⋮ , **View**.

2

Click on the view you want to display.

End of steps

1.4 How do I work in a view?

Typically, an operator is assigned to actively monitor one or more views. In a view, the supervision groups that belong to the view are shown as tiles in a grid. The color of the tiles indicates the relative health of the NEs in the group, based on KPIs such as number of alarms or affected objects. Tile position also indicates health; groups with the most problems are in the upper left.

The KPI information and tile position are updated at a user-configured trend time interval. If KPIs for a group have become worse since the last interval, a trend arrow is displayed in the upper right of the group tile. In a view, you can see at a glance which supervision groups need investigation or troubleshooting.

In a view, you can perform the following:

- View additional information for a supervision group: hover over **More** and click **More Details** to expand the group tile. The expanded tile displays the number of alarm-affected cards, ports, and links in the group, as well as the number of acknowledged and unacknowledged alarms.
- View all current alarms for a supervision group: hover over **More** and click **Current Alarms** to open an alarm list for the group.
- View the contents of a supervision group: double-click on the group tile. The NEs in the group are displayed in one of the supervision group display formats; see 1.8 “What are the supervision group display formats?” (p. 11).

  When you open a supervision group in any display format, a Group Access Drawer becomes available on the left. You can hover on the group icons in the Group Access Drawer to see group status and KPIs, and you can click on an icon to open that group.

1.5 How does access control affect objects in Network Supervision?

An operator’s visibility of network equipment is based on access control settings, which are configured by an administrator. Depending on your access settings, some equipment may not be visible. See the User Manager Application Help and your network administrator for more information.

1.6 Task flow: How do I set up and optimize Network Supervision?

You can customize the Network Supervision application to suit your network monitoring requirements. The following task flow describes preliminary steps for organizing network equipment, and for setting preferences for displays, refresh rates, statistics collection, and other customizations.

1

Using the Group Manager application, create supervision groups and views to organize your network equipment. The Group Manager application requires a user with administrator privileges.

2

If required, use the Group Manager application to configure a physical map layout for the Topology view to define regions, zones, and subzones. The Group Manager application requires a user with administrator privileges.

3

If required, add a geographical background map for the Topology view. Map backgrounds are configured by an administrator, using the System Settings option under User, Settings on the NSP Launchpad. See the *NSP System Administrator Guide* for more information about NSP system settings.

4

Set preferences for the following:

- Application preferences; see 1.26 “How do I configure application preferences?” (p. 29).
- KPI threshold settings; see 1.27 “How do I configure KPI threshold settings?” (p. 29).
- Event Timeline settings; see 1.28 “How do I configure Event Timeline settings?” (p. 30) and 1.22 “Assurance event recording and retrieval in Network Supervision” (p. 25).
- User preferences for view capacity, sorting, and trend time interval (refresh rate); see 1.29 “How do I configure user preferences?” (p. 30)
- Utilization Map settings; see 1.30 “How do I set Utilization Map preferences?” (p. 31)

5

For the Topology view, numerous display settings are available. Some, like physical map layout and map background, are set by an administrator. Others, like cluster controls, are set by the operator using the map; see 1.10 “How do I work in the Topology Map?” (p. 12).

1.7 Sample task flow: How do I use Network Supervision for active monitoring?

Network Supervision allows you to actively monitor your network to identify equipment problems at a high level, and then drill down to specific NEs to investigate further.

The following task flow describes a typical process for active monitoring to identify, troubleshoot, and resolve network equipment problems.

1

Choose a view; see 1.3 “How do I change the view?” (p. 7). A view provides a high-level overview of KPIs for the supervision groups that it contains.

2

Within the view, identify supervision groups with the highest-priority problems; see 1.4 “How do I work in a view?” (p. 8).

3

Choose a supervision group for further investigation.

4

Choose a display format for the supervision group; see 1.8 “What are the supervision group display formats?” (p. 11).

5

Based on information presented in the chosen display format, triage within the supervision group to identify NEs with high-priority problems that need further investigation.

6

Choose an NE, and select a troubleshooting tool.

There are three main troubleshooting tools, each of which launches a task flow for closer investigation of the problem:

- Current Alarms list; see 1.19 “How do I work with the Current Alarms list?” (p. 23).
- Event Timeline; see 1.20 “How do I work with the Event Timeline?” (p. 24).
- Troubleshooting Map; see 1.21 “How do I work with the Troubleshooting Map?” (p. 24).

Use the tools to investigate root causes and impacts, to identify a specific problem on a specific equipment object.

7

If possible, make the required fixes using the management application for the NE.

8

Add the NE to the Watch Drawer for follow-up observation, if required.

9

Investigate other NEs in the selected supervision group, as required.

10

Return to the view for active monitoring at the highest level.

1.8 What are the supervision group display formats?

When you select a supervision group from a view for further investigation, you can choose from various display formats that show different information and perspectives on the equipment or links in the supervision group.

Network Supervision provides the following display formats for supervision groups:

- **Matrix View**; see 1.9 “How do I work in the Matrix view?” (p. 11)
- **Topology View**; see 1.10 “How do I work in the Topology Map?” (p. 12)
- **Multi-Layer View**; see 1.15 “How do I work in the Multi-Layer view?” (p. 20)
- **NE List**; see 1.16 “How do I work in the NE List?” (p. 21)
- **Link List**; see 1.17 “How do I work in the Link List?” (p. 22)

The different display formats help you to find and identify different types of problems on NEs, then navigate to specific objects for further investigation and troubleshooting. For example, the Matrix view uses tiles in a grid to show equipment KPIs, such as number of alarms and number of affected cards and ports. Map views display NEs and links in a topology, to show the relationships between network objects. List views show detailed information, and allow sorting and filtering of large volumes of data.

To change the display format, click the Format Changer in the upper right corner of the page and select a format from the list:

A search function is available in all display formats. Click **Search** to search for physical equipment and VNFs, based on different attributes, such as name or location.

1.9 How do I work in the Matrix view?

The Matrix view displays NEs as tiles that show basic information about hardware status for the NE (similar to the view display, but showing information at the NE level rather than the supervision group level). Tile banner color indicates the amount of affected equipment on the NE, based on KPI threshold settings. Tile position also indicates health; NEs with the most problems are in the upper left.

The KPI information and tile position are updated at a user-configured trend time interval. If KPIs for a group have become worse since the last interval, a trend arrow is displayed in the upper right

of the group tile. These high-level visual cues help identify NEs with the most serious problems, so you can identify where to investigate first.

To investigate NE problems, the Matrix view allows you to perform the following:

- View additional details for an NE: click **Show More**, **More Details**. The tile expands to display additional alarm, status, software version, and physical location information for the NE.
  Note: Some of the fields in More Details are not applicable to Private Wireless (SBTS) NEs, and can be ignored.
- View current alarms for an NE: hover over **Show More** on a tile and click **Current Alarms** .
- View the event timeline diagram for an NE: hover over **Show More** on a tile and click **Event Timeline**.
- View an NE in a troubleshooting map: hover over **Show More** on a tile and click **Troubleshooting Map**.
- View the equipment inventory for an NE: click **Show More**, **Equipment Inventory**.
- Add the NE to the Watch view: click **Show More**, **Add to Watch View**.
- View merged alarms for an NE: click **Show More**, **Merged Alarms**.
- View historical alarms for an NE: click **Show More**, **Historical Alarms**.
- View an NE in its management application: click **Show More**, **Show Object**. The object is opened for configuration in its management application.
- Open an SSH or Telnet session for the NE: click **Show More**, **Open NE Session**. See 1.31 “How do I open an SSH or Telnet session with an NE?” (p. 31).
- View an NE in its web application or element management system: click **Show More**, **Show External EMS**. This option is available for Wavence devices using the CorEvo card.
- Run Analytics reports for an NE: click **Show More**, **Analytics**. Select **Inventory Reports**, **Utilization Reports**, or **OAM Reports** from the sub-menu.

1.10 How do I work in the Topology Map?

The Topology View displays the NEs in a supervision group as a map of linked objects. Physical topology maps can display either an Operational map view or a Utilization map view. The Operational view is displayed by default.

Physical Map Layout

Supervision groups may be administratively enabled for Physical Map Layout. Physical Map Layout allows NEs to be grouped into regions, and further subdivided into zones and subzones. Region and zone groupings provide the basis for clustering map objects when region-based clustering is enabled for a map.

Topology maps with Physical Map Layout may show a geographical map as a background, and the icons for regions, zones, or NEs may be placed on the background map to reflect their actual geographical location.

When objects share the same physical location, the map shows a stacked icon shaded blue. Click **Legend**, **Vertex Types** for more information. To see the co-located objects individually, drag them off the stack.

Physical Map Layout settings are configured by an administrator with the required permissions. Regions and zones are configured using the Group Manager; see the Group Manager Help. Map backgrounds are configured through the NSP system settings, accessed from the NSP Launchpad; see the *NSP System Administrator Guide*.

Topology View functions

The Topology View allows you to perform the following:

- Switch map views: the Operational map is the default view. To switch to the Utilization view, click  **View**, **Utilization**.
- View quick NE information: hover over an NE or link object to display basic system and alarm information for the object.
- View full NE details: click **Info** to open the Information panel, which displays detailed information about a selected map object.
- Interpret map information: click **Legend** to open the map legend, which describes the meaning of different objects, link media types, and status colors seen in the topology map.
- Highlight links to identify by type: click **View Options** to open the Link Highlight Options panel. Click on the icons to highlight various link types. See 1.35 “How do I highlight links by type in the Topology View? ” (p. 34) for more information.
- Find alarm-affected NEs: NE objects with alarms carry a badge. The badge color indicates alarm severity, as described in the Legend panel.
- Filter the topology map content: use filters to control the display of information and reduce clutter; see 1.34 “How do I filter the Topology View?” (p. 33).
- Refresh map data: click **Refresh Data** to update the map contents.
- View a map object in its management application: click on the NE or link object you want to view. In the Information panel, click **More actions**, **Show Object**. The object is opened for configuration in its management application.

  For NSP deployments that include NRC-X, click on a cross-domain link and select **More**, **Show in Cross Domain Coordinator**. The Cross Domain Coordinator application opens with the cross-domain link highlighted on the network map.
- Open an SSH or Telnet session for the NE: click on the NE in the map, then click **Info** to open the Information panel. Click **More actions**, **Open NE Session**. See 1.31 “How do I open an SSH or Telnet session with an NE?” (p. 31).
- View a list of optical services for cross-domain links: click on the cross-domain link you want to view. In the Information panel, hover over the **More Actions** button for a link, then select **Show Optical Services**. A list of optical services that terminate on the optical endpoint of the cross-domain link is displayed.
- Control the map display: click on the icons in the map controls panel to perform the following:
  - **Fit to screen** . Fit the map to the available screen area.
  - **Adjust clustering** . Reduce the number and density of NE objects on the map by combining NEs into clusters that show a single icon. Cluster icons are square with rounded corners. See 1.36 “How do I manage clusters in the Topology View? ” (p. 35) for information about clustering controls.
  - **Adjust vertexes** . Show or hide text labels for vertexes, adjust vertex size, and show or hide connectors to vertexes (NEs) in other supervision groups that are external to the current

supervision group displayed on the map. When **Show connectors** is enabled, you can control the level of detail for connectors to those external vertexes. For more detail, choose the **To vertex** option; the map displays connectors to all vertexes outside the group. For less detail, choose the **To group** option to show a single connector to any external supervision groups. When Show connectors -To group is enabled, you can navigate to the external group by double-clicking on its icon.

- **Adjust links** . Show or hide links, adjust link curvature, specify the link grouping threshold, and show health indicators for link groups, either as a pie chart or a solid color. Group health indicators show the color of the most severe status of links in a group. Pie charts show the percentage of links with the most-severe status (but for very small percentages, a minimum of 12% is displayed for visibility). The order from most to least severe for link status is Failure, Maintenance, Unknown, Normal. See the Legend for link status colors.
- **Map view** . Show a bird`s eye view of the map.
- **Zoom controls** . Zoom in and out on the map.

- Change, save, and restore layouts: drag map objects to change their placement on the map. Save the new layout, or restore the map to the common layout set by an administrator. See 1.37 “How do I save and restore layout changes in the Topology View?” (p. 36).
- Find NEs in the map: see 1.38 “ How do I find NEs in the Topology View?” (p. 37).

1.11 How do I remove disabled LLDP links from the Topology Map?

Disabled LLDP links that are managed via the LLDP application do not disappear automatically from the Topology Map. They are persisted in red. Administrative users can remove these disabled LLDP links from the Link List view.

1

In the Network Supervision GUI, select the **Link List** display format.

2

In the Link List, click **Delete** on the physical link item you want to remove.

You can filter the list to show only disabled links: select Disabled under the Operational State column. You can also search for an individual link ID under the Link Name column.

The Delete icon is only enabled on disabled links.

END OF STEPS

1.12 How do I check link usage in the Topology Map?

You can switch the Topology Map and Troubleshooting Map to the Utilization option to show how much of the capacity is being utilized on network links. Utilization is displayed as colored arrows on link objects. When you hover over a link, its utilization level is displayed in the object tooltip. You can also view a link’s utilization data in the Info panel: select a link on the map and click **Info**. Click on the link item in the Info panel to expand it and look for link/endpoint utilization data.

For more information about the Utilization map view option, see 1.13 “What is the Utilization map option?” (p. 14).

To switch to the Utilization map view option:

- Click View Utilization **View**, **Utilization** within the Topology View or Troubleshooting Map.
  Region and zone icons cannot be opened while in the Utilization view. For full navigation, you must switch back to the Operational view.

Note: If an MC LAG link switchover occurs while you are viewing the Utilization map, the change will not appear in the map unless you switch to the Operational view and then switch back to Utilization.

1.13 What is the Utilization map option?

The Topology Map and Troubleshooting Map have a Utilization view option that shows how much available capacity is being utilized on network links. The Utilization view lets you quickly assess how efficiently your network is managing traffic, and identify links that are over- or under-utilized. Utilization is displayed as colored arrows on link objects. Network utilization can be analyzed in the Topology Map for all links in a supervision group, and in the Troubleshooting Map for a focused set of links.

The Utilization view option supports a limit of five active users at any one time. If more than five users access the Utilization view, a notification is displayed.

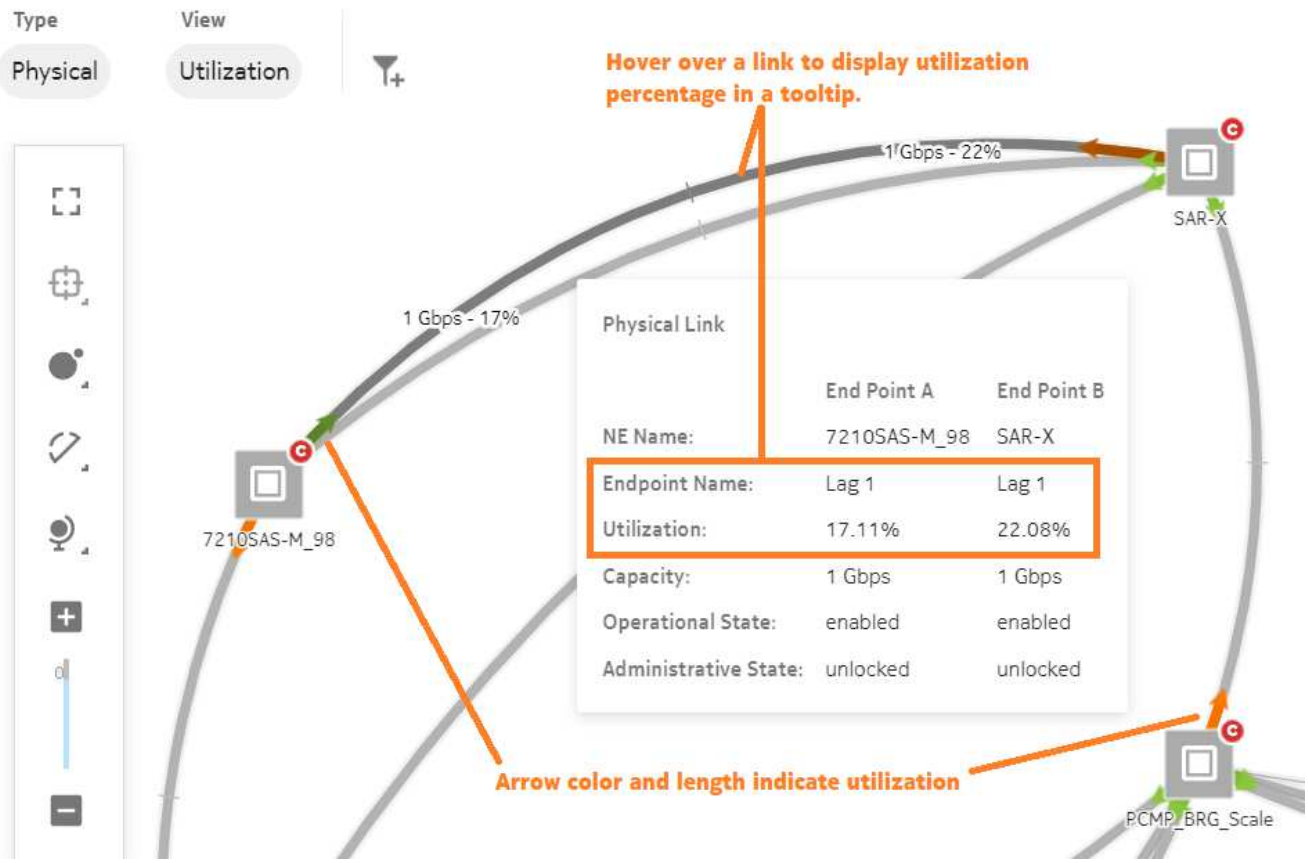
Information in the Utilization view is based on port egress statistics collected for IP links on Ethernet physical ports. Statistics must be supported and available for utilization to be displayed; see 1.14 “Utilization map statistics collection” (p. 18).

The Utilization view displays usage data for the following link types:

- Point-to-Point (IP / IGP / CUPS)
- LAG
- Cross-domain
- Radio microwave
- Optical

The Topology view shows the Operational map by default. To switch to the Utilization map option, click View Utilization **View**, **Utilization** within the Topology View or Troubleshooting Map.

The Utilization view option supports physical map layout and region-based clustering, but region and zone icons cannot be opened while in the Utilization view. For full navigation, you must switch to the Operational view.



The Utilization Map shows NEs connected by link lines that represent physical connections between endpoints. When you hover over a link, its utilization level is displayed in the object tooltip. The links have the following features:

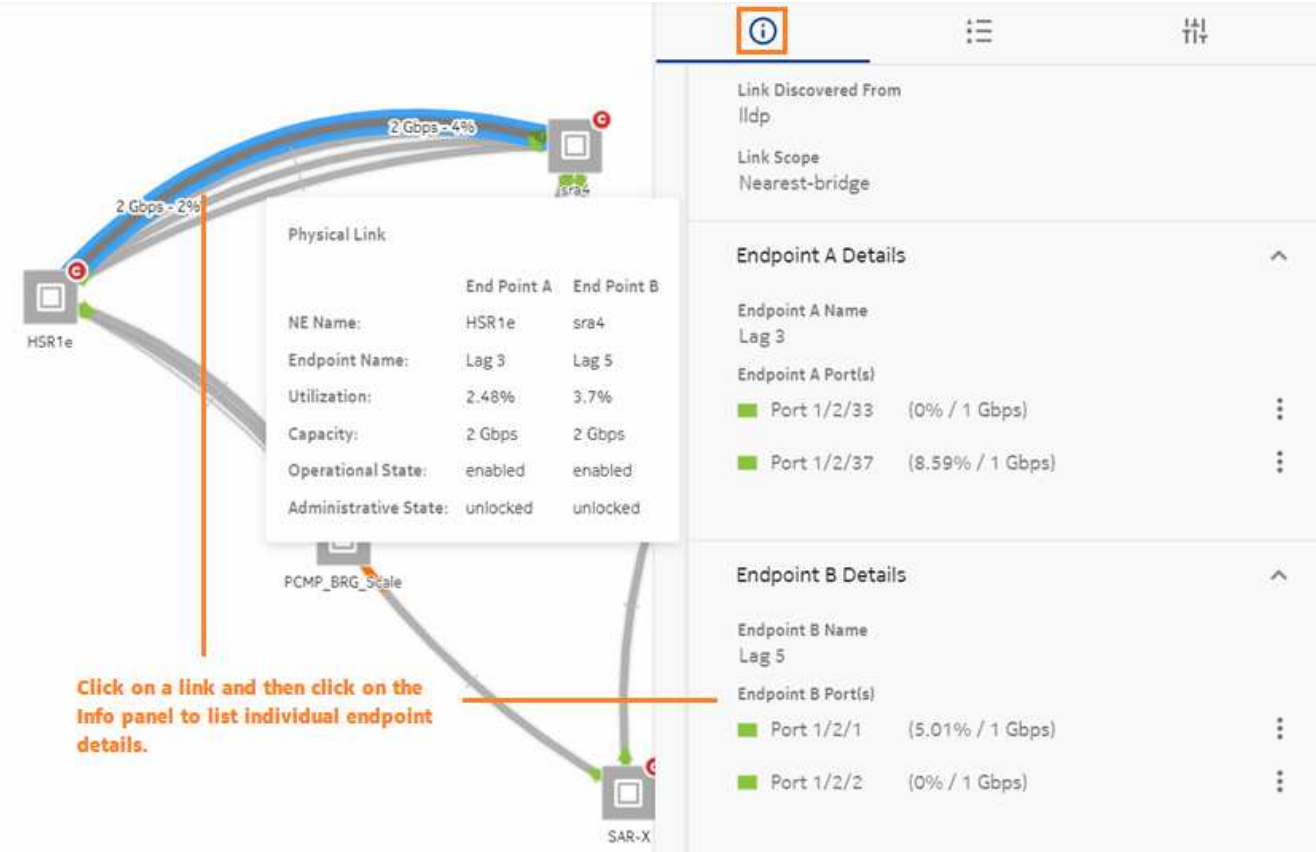
- **Thickness**. The relative capacity on the link is indicated by a thin, medium, or thick line. Thinner lines indicate lower capacity, thicker lines indicate higher capacity. Link capacity is based on the operational port speed configured for the port.
- **Color**. Physical links between endpoints are shown in grey. Utilization is shown as a green, orange, or red arrow along the grey line. Each color indicates a range of utilization: low, medium, or high. The colors change as utilization (in percent) crosses preset thresholds.
- **Arrow length**. The length of the colored arrow shows the relative utilization of the capacity on the link. Arrows grow from minimal utilization at an endpoint, to 100% utilization at the mid-point crossbar (for bidirectional links). The crossbar represents 100% utilization from either direction.

  Utilization rates near zero will show a disproportionately long arrow (it may look like about 5%) to provide a visual cue that there is utilization on the link.

  A grey line with no colored arrow means either zero utilization, or there is no data available for that link.

  If utilization statistics are not supported on an NE, traffic may be present, but no utilization arrow is displayed.

You can click on a link and display detailed information relating to links and individual endpoints on the Info panel.



You can filter the Utilization view content to show specific information; see 1.34 “How do I filter the Topology View?” (p. 33).

You can set your own preferences for the map refresh rate. To modify appearance change thresholds for port speed (line thickness) and utilization percentage (arrow color); see 1.30 “How do I set Utilization Map preferences?” (p. 31).

Note: The size of the supervision group may affect performance. Consider the following:

- If the number of links in the supervision group is large, there may be a delay before the Utilization option appears in the View menu.
- Statistics are collected by subscription from qualified ports. If there are too many qualified ports in the supervision group, performance may be affected. For information about Utilization map scale limits, see the *NSP Planning Guide*.

1.13.1 Managing link utilization map performance

To maintain system performance and to avoid exhausting available statistics counters, consider creating groups of no more than 50 NEs for the purpose of link utilization monitoring. Assemble the groups in the NSP Group Manager application as described in the NSP Group Manager Application Help and then select a group for monitoring in Network Supervision.

Be aware that Utilization map performance can also vary based on the number of subscriptions and on other telemetry gathering on the NSP system.

1.14 Utilization map statistics collection

Information in the Utilization map is based on port egress statistics collected for IP links on Ethernet physical ports. Statistics must be supported and available for utilization to be displayed. The Operational State of NEs and ports must be Up.

Utilization statistics are collected from NEs using SNMP for NFMP NEs and gRPC for MDM NEs.

When a user switches from the Operational Map to the Utilization Map, the first two telemetry subscriptions listed below are created. If LAG links are present on the map, the third subscription listed below is created.

1. Subscription for SNMP and MDM managed NEs and ports on the current map.

   SNMP-managed 7750 SR family NEs respond to the filter.

   The following MDM-managed NEs respond to the filter: 7750 SR, 7250 IXR / VSR(I), 7450 ESS, and 7950 XRS

   This subscription determines utilization directly from the output-utilization statistic counter.

2. Subscription for SNMP managed 7705 SAR and 7210 SAS NEs and ports on the current map.

   This subscription calculates utilization from the following statistics: operational-speed, transmitted-broadcast-packets-periodic, transmitted-multicast-packets-periodic, transmitted-octets-periodic, and transmitted-unicast-packets-periodic.

   SNMP utilization statistics are calculated from NFM-P counters using this formula:

   ```
   output-utilization(%) = (transmittedTotalOctetsPeriodic +
   ((transmitted-unicast-packets-periodic +
   transmitted-multicast-packets-periodic +
   transmitted-broadcast-packets-periodic) * 20)) *
   8/t/operational-speed/1000 * 100
   ```

   Where **t** is the collection interval in seconds, as specified in the Utilization Map preferences.

3. Subscription for SNMP-managed NEs and LAG links on the current map.

   This subscription calculates utilization from the following statistics: speed, transmitted-broadcast-packets-periodic, transmitted-multicast-packets-periodic, transmitted-octets-periodic, and transmitted-unicast-packets-periodic.

   SNMP utilization statistics are calculated from NFM-P counters using this formula:

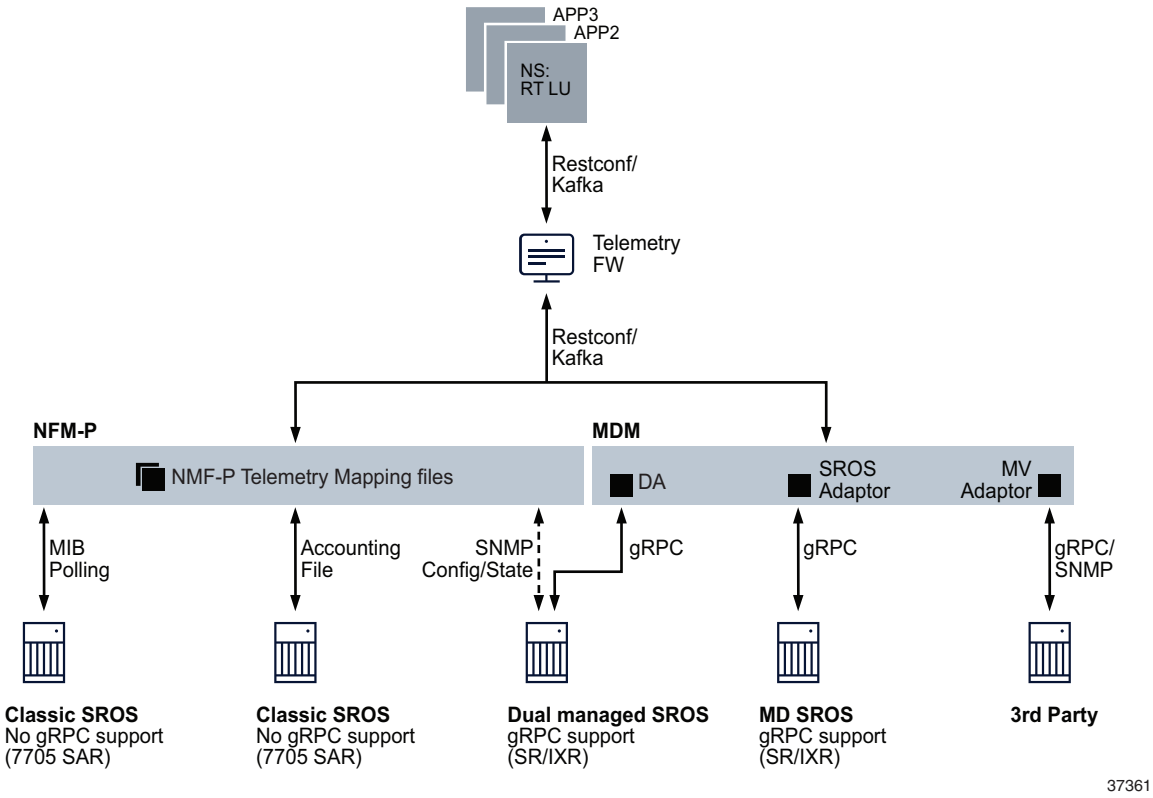
   ```
   output-utilization = (transmitted-octets-periodic +
   ((transmitted-unicast-packets-periodic +
   transmitted-multicast-packets-periodic +
   ```

```
transmitted-broadcast-packets-periodic) * 20)) *
8/t/operational-speed/1000 * 100
```

Where **t** is the collection interval in seconds, as specified in the Utilization Map preferences.

The figure below describes the telemetry data collection process from classic NFM-P and MDM managed NEs for the utilization map.

Figure 1-1 Utilization data collection



For SNMP, NEs must be managed by the NFM-P and reachable using SNMP. The following are used for utilization data:

- MIB name: TIMETRA-PORT-MIB
- MIB entry name: tmnxPortEtherEntry
- MIB counter name: tmnxPortEtherUtilStatsOutput
- Statistics group: Additional Ethernet Stats
- Counter: utilStatsOutput (in centi-percent)

The following NEs support the required SNMP statistics for the Utilization map:

- 7250 IXR

- 7450 ESS
- 7750 MG and MG VSR
- 7750 SR and VSR
- 7950 XRS

For MDM, the following gRPC schema path is used for utilization data:

- /state/port[port-id]/ethernet/statistics/out-utilization

SR OS NEs support the required MDM statistics for the Utilization map. The supporting chassis types are:

- 7250 IXR
- 7450 ESS
- 7750 MG
- 7750 SR
- 7950 XRS

1.14.1 Utilization statistics for the 7705 SAR and 7210 SAS

The following (periodic) counters are used for utilization calculation for the 7705 SAR and 7210 SAS:

- MIB name: IF-MIB
- MIB entry name: ifXEntry
- MIB counter names: ifHCOutOctets, ifHCOutUcastPkts, ifHCOutMulticastPkts, ifHCOutBroadcastPkts
- NFMP statistics group: Interface Additional Statistics
- NFMP counters: transmittedBroadcastPackets, transmittedMulticastPackets, transmittedTotalOctets, transmittedUnicastPackets

The following information is used to establish a reference speed:

- MIB name: TIMETRA-PORT-MIB
- MIB entry name: tmnxPortEtherEntry
- MIB counter name: tmnxPortEtherOperSpeed (mbps)
- NFMP class: equipment.PhysicalPort
- NFMP counter: actualSpeed (kbps)

1.15 How do I work in the Multi-Layer view?

The Multi-Layer View shows the relationships between equipment objects in various layers of the network; for example, the physical layer and the IGP layer. The IGP layer is displayed for physical

NEs contained in a single supervision group where the corresponding IP links and routers can span over multiple administrative domains. You can see how problems in one layer may be affecting, or affected by, other layers.

The Multi-Layer map allows you to perform the following:

- Refresh map data: click **Refresh Data** to update the map contents.
- Search the map: click **Search** to search for objects based on different attributes, such as name, or location.
- View full NE details: click **Info** to open the Information panel, which displays detailed information about a selected map object.
- Interpret map information: click **Legend** to open the map legend, which describes the meaning of different objects and status colors seen in the map.
- Configure view options: click **View Options** to show or hide the IGP and physical layers.
- Save layout changes: click **More**, **Save as My Layout** to save your layout settings for the current session and subsequent sessions.
- View a list of optical services for cross-domain links: click on the cross-domain link you want to view. In the Information panel, hover over the **More Actions** button for a link, then select **Show Optical Services**. A list of optical services that terminate on the optical endpoint of the cross-domain link is displayed.
- Open an SSH or Telnet session for the NE: click on the NE in the map, then click **Info** to open the Information panel. Click **More Actions** , **Open NE Session**. See 1.31 “How do I open an SSH or Telnet session with an NE?” (p. 31).
- Control the map display:

  Click on the icons in the map controls panel to perform the following:
  - **Fit to screen** . Fit the map to the available screen area.
  - **Adjust vertexes** . Show or hide connectors and show or hide text labels for vertices.
  - **Adjust links** . Show or hide links and specify the link grouping threshold.
  - **Map view** . Show or hide layer labels, show/hide cross-layer columns, set layer spacing and layer opacity.
  - **Zoom controls** . Zoom in and out on the map.

1.16 How do I work in the NE List?

The NE List displays NEs as items in a list table, with columns showing system information for the NE. You can filter and sort the list to reduce a large amount of data, to show only the information you need.

- View current alarms for the supervision group: click **Current Alarms** on the toolbar. To return to the list, click **Object View**.
- Filter the NE list under a specific column: type a text string in the text field at the top of a column and press Enter. Click **Clear Filter** to clear column filters.
- Sort the NE list under a specific column: click on a column header to sort the list under that column. Click the column header a second time to toggle the sort order (ascending/descending), as indicated by the Up/Down arrow.

- View current alarms for an NE: hover on an NE in the list and click **Current Alarms**.
- View the event timeline diagram for an NE: hover on an NE in the list and click **Event Timeline**.
- View the NE in a troubleshooting map: hover on an NE in the list and click **Troubleshooting Map**.
- View the equipment Inventory for an NE: hover on an NE in the list and click **More**, **Equipment Inventory**.
- View merged alarms for an NE: hover on an NE in the list and click **More**, **Merged Alarms**.
- View historical alarms for an NE: hover on an NE in the list and click **More**, **Historical Alarms**.
- Add an NE to the Watch view: hover on an NE in the list and click **More**, **Add To Watch View**.
- Open an NE in its management application: hover on an NE in the list and click **More**, **Show Object**.
- Open an SSH or Telnet session for the NE: hover on an NE in the list and click **More**, **Open NE Session**. See 1.31 “How do I open an SSH or Telnet session with an NE?” (p. 31).
- Run Analytics reports for an NE: hover on an NE in the list and click **More**, **Analytics Reports**.
- Copy NE information to the clipboard: hover on an NE in the list and click **More**, **Open In Copy Window**. In the Copy window, press Ctrl+C or Command+C.

Note: In a dual NE management scenario, in which MDM is used for telemetry and NFM-P is used for everything else, if IPv6 is enabled, MDM reads the IPv6 address as the NE ID. Network Supervision would display the same NE as two objects.

1.17 How do I work in the Link List?

The Link List shows a table of information about physical links in a supervision group. Each row of the table shows information for one physical link. The operational state of the link, and information about both endpoints (A and B), are displayed.

The Link List allows you to perform the following:

- Filter and sort the list: use the same filtering and sorting functions as other NSP list formats; see 1.16 “How do I work in the NE List?” (p. 21).
- Investigate alarms: click **Current Alarms** on the toolbar.
- Refresh the list: click **Refresh List** on the toolbar.
- Open a troubleshooting map for a link: hover on a list entry and click **Troubleshooting Map** at the far right. The Troubleshooting Map highlights the link and shows the two endpoint NEs, plus one hop from each endpoint. The Hop count and Explore functions are supported; see 1.21 “How do I work with the Troubleshooting Map?” (p. 24).
- Open a list of optical services for cross-domain links: hover over a cross-domain link in the list and click **More Actions** , **Show Optical Services**. A list of optical services that terminate on the optical endpoint of the cross-domain link is displayed.

- Click **Delete** on a disabled physical link item you want to remove. The Delete icon is only enabled on disabled links.

1.18 What is the Equipment Inventory?

The equipment inventory tree allows you to quickly locate affected NE objects (NEs, LAGs, shelves, slots, cards, ports). Affected NE child objects are displayed in an expandable/collapsible hierarchy. The color of an inventory object indicates its state. The various state-colors are described in the Legend.

- Expand all objects: click **Expand All** on the view header to expand all objects in the Equipment Inventory view, down to the lowest child object level.
- Collapse all objects: click **Collapse All** on the view header to collapse the Equipment Inventory view, up to the parent NE object level.
- View full object details: click **Info** to open the Information panel, which displays detailed information about a selected inventory object.
- Interpret inventory information: click **Legend** to open the inventory legend, which describes the meaning of different objects and status colors seen in the inventory.
- Filter the equipment inventory: click **Add Filter** to display only specific objects in the Equipment Inventory view. Select one of the filter types: Type, Operational State, or Administrative State.

  A chip filter is added to the inventory. Click on the chip filter and select one or more criteria related to the filter type. Click **Close** on a chip filter to remove it from the map.
- Refresh data: click **Refresh Equipment** to update the inventory contents. The equipment inventory is refreshed automatically when Auto Refreshing is enabled.

1.18.1 Inventory objects

Individual inventory objects (child objects) show basic administrative and operational state information. Click on an inventory object to show additional details in the Information panel.

- Expand an inventory object: click **Expand All** on an inventory object to expand all child objects to the object.
- Configure an inventory object: click **Show Object** on an inventory object to open a management application configuration form for the object.

1.19 How do I work with the Current Alarms list?

Alarms against equipment are displayed in the Current Alarms list. From the list, you can clear alarms, perform impact analysis, and access links to view detailed alarm information and take corrective action.

Access the alarm list by clicking **Current Alarms** in the NE Matrix, NE List, or Link List formats, or in the Watch view. Alarm information is also available from the Utility drawer.

For more information about alarm lists see the Fault Management application help.

1.20 How do I work with the Event Timeline?

The Event Timeline shows alarms, configuration changes, and software updates on the NE as events in a time sequence. You can drill down in the timeline to specific events, and view information about those events. You can see which events are root causes, and then access more details to confirm. The range of time for the timeline is user-configurable from within the Event Timeline display. Event Timeline is a useful tool for identifying state changes and configuration events, especially when used in conjunction with alarms.

Access the Event Timeline by clicking **Event Timeline** in the NE Matrix or NE list formats, or in the Watch view.

Perform the following tasks in the Event Timeline:

- Set a date range: click **Select Date Range** and choose the start and end dates for which events will be shown.
- Show event details: click on an event on the timeline and click **Event Details** to view information related to the event.
- Zoom in on clustered events: click the **Zoom** buttons to expand or collapse event clusters.

  You cannot set the zoom level below a 10 ms interval, which may leave some events clustered.
- Scroll along the timeline: click the **Move Right/Left** buttons to move forward and backward along the timeline.

For information about how events are recorded and retrieved, see 1.22 “Assurance event recording and retrieval in Network Supervision” (p. 25).

1.21 How do I work with the Troubleshooting Map?

The Troubleshooting map allows you to investigate a specific NE and its immediate neighbors in the network. It shows a topology of the selected NE and links to any connected NEs, up to a user-defined number of hops away. This is useful for root cause and impact analysis, since problems on one NE often affect neighboring NEs.

The Troubleshooting Map is available for specific NEs using the **More** menu for the NE object in the Matrix View, NE List, and Link List formats, and in the Watch view.

The Troubleshooting Map allows you to perform the following:

- Switch map views: the Operational map is the default view. To switch to the Utilization view, click **View**, **Utilization**. See 1.13 “What is the Utilization map option?” (p. 15) for more information.
- Set number of hops from initial object: set the **Hop count** to show NEs and links a specified number of hops from the initial NE (to a maximum of five hops).
- View quick NE information: hover over an NE or link object to display basic system and alarm information for the object.
- View full NE details: click **Info** to open the Information panel, which displays detailed information about a selected map object.
- Interpret map information: click **Legend** to open the map legend, which describes the meaning of different objects and status colors seen in the topology map.

- Refresh map data: click **Refresh Data** to update the map contents.
- View a map object in its management application: click on the NE or link object you want to view. In the Information panel, click **More**, **Show Object**. The object is opened for configuration in its management application.

  For NSP deployments that include NRC-X, click on a cross domain link and click **More**, **Show in Cross Domain Coordinator**. The Cross Domain Coordinator application opens with the cross domain link highlighted on the network map.
- Open an SSH or Telnet session for the NE: click on the NE in the map, then click **Info** to open the Information panel. Click **More actions**, **Open NE Session**. See 1.31 “How do I open an SSH or Telnet session with an NE?” (p. 31).
- Control the map display. Click on the icons in the map controls panel to perform the following:
  - **Fit to screen** . Fit the map to the available screen area.
  - **Adjust vertexes** . Adjust vertex size, show or hide connectors, and show or hide text labels for vertexes.
  - **Adjust links** . Show or hide links, adjust link curvature, turn link grouping on or off, and specify the link grouping threshold.
  - **Map view** . Show a bird`s eye view of the map.
  - **Zoom controls** . Zoom in and out on the map.

1.22 Assurance event recording and retrieval in Network Supervision

Assurance events are used in the Network Supervision application as a troubleshooting tool to give the user insight into the events that led to a certain state. For example, an operator could examine events that occurred on an NE or service prior to a critical alarm and see if there was a configuration change that resulted in an alarm.

Assurance events are sequential historical events recorded on NE or service objects and their hierarchical sub-components. The type of events that can generate an assurance event are:

- object creation, including alarm creation (AlarmRaised)
- attribute change, which can include configuration change (ConfigurationChange) and state change (StateChange), depending on which attributes have changed
- object deletion, including alarm deletion (AlarmCleared)
- alarm update

1.22.1 Assurance event recording in NFM-P

Assurance events for NFM-P-managed objects are recorded using NFM-P event generation (JMS). The assurance event recorder subscribes to the JMS events. If an event is on an object of interest, it is translated into an assurance event record and logged using the event logging framework.

The assurance event logging framework provides an application-agnostic recording interface. By default, assurance events are recorded in an Oracle database, but if the customer has configured an auxiliary database, the recording is automatically routed to the auxiliary database.

An NFM-P Event policy allows you to enable/disable event recording (Admin State Up/Down) and the log retention time. To configure an Event policy, open the NFM-P GUI, click **Tools** menu, **Events**, **Event Policies**. The framework also provides tools to purge events.

Event log retention time defaults and minimum/maximum values depend on the type of database you are using.

Table 1-1 Event log retention time defaults and minimum/maximum values

Database type	Default retention time	Minimum retention time	Maximum retention time
Oracle	168 hours (one week)	One hour	720 hours (1one month)
Auxiliary	720 hours (one month)	One day	8760 hours (one year)

In addition to NFM-P Event Policy configuration, you must enable event recording in the Network Supervision Timeline Settings form. Click ⋮ **More**, **Timeline Settings**. You can enable event recording for specific application objects:

Table 1-2 Network Supervision objects with event recording

Object type	NFM-P class
Network Element	netw.NetworkElement
Link	netw.AbstractPhysicalLink
Card	equipment.Card
Port	equipment.Port
Site	rtr.ProtocolSite
Network Interface	rtr.NetworkInterface
LAG Interface	lag.Interface
Site Sync	sonet.SiteSync
MPLS	rsvp.Interface
IGP	isis.Interface
IGP	ospf.Interface
VNF Instance	nfv.VNFInstance
VNF Component	nfv.VNFComponent

1.22.2 Assurance event recording in NSPOS

For objects managed by MDM or NFM-T, event logging is implemented using time series model recording.

You enable event logging globally for NSP from the NSP Launchpad. Click **User**, **NSP Settings**, **Event Logging Policy**. This setting is for NSP event logging only. It applies to non-NFM-P-managed objects.

The assurance event framework detects changes on common model objects by listening to corresponding **`nsp-db-<model>`** topics (e.g., **`nsp-db-equipment`**, **`nsp-db-service`**, **`nsp-db-alarm`**) which report any change committed to the common model database. If the change is detected on any one of the pre-configured objects, the application creates an assurance event and publishes it to a Kafka topic. The nspos-ts-data-manager-app listens for assurance events from applications and adds them to the ts.AssuranceEvent table.

1.22.3 Assurance event format

Each NFM-P or NSPOS event contains the following information:

Table 1-3 Assurance event information components

Event component	Description
managedObjecFdn	Derived FDN of the ancestor MO to the MO that generated the event (e.g., Service FDN).
eventFdn	FDN of the MO that generated the event (e.g., Site FDN).
creationTime	Event creation time.
eventType	Can be any of: AlarmRaisedEvent, AlarmUpdateEvent, AlarmClearedEvent, CreationEvent, ConfigurationEvent, StateChangeEvent, DeletionEvent, TestFailureEvent, AnomalyEvent, ThresholdCrossedEvent, ScaleOutEvent, ScaleInEvent, HealingEvent, CustomEvent, UpgradeEvent, CustomOperationEvent, InstantiateEvent
eventRecord	json-encoded event data.

1.22.4 Assurance events retrieval

The Assurance application retrieves events from the appropriate database (NFM-P or NSPOS), based on the original source of the object.

Assurance events are retrieved using API commands from the web component library (assurance-share-md), which provides web components to display events on a timeline. Assurance events are recorded and stored on a server that is accessible from the Network Supervision application using the web component library.

The web component library provides:

- Retrieve events from the NFM-P or NSPOS database, based on the source of the referenced object.
- Display events in a timeline view. Events are grouped into categories in the display, and multiple categories are presented on the same event timeline.
- Ability to filter assurance events based on the source object type or category.

- Ability to select individual events and examine event details.
- Ability to select a set of events to form a pattern, and then searching the Event Timeline for a similar pattern of events.

The Event Timeline will display events for multiple objects at the same time if all of the selected objects are part of the same object hierarchy, and all of the objects are at the same level in the hierarchy (for example, multiple service sites for the same service).

By default, events from the last 24 hours are retrieved. You can specify a different time window using the **Select Date Range** tool on the Event Timeline.

1.23 What are cross-domain links?

Network supervision provides visibility of cross-domain links between IP and optical equipment. Cross-domain links are shown on topology maps as dashed lines, and on multi-layer maps as solid lines. They are also included in the Link List.

For cross-domain links, you can access a list of optical services that terminate on the optical endpoint of the link. The list shows information about those optical services, and provides additional options. A list of optical services is available from the Topology View, Multi-Layer View, and Link List formats; see 1.33 “How do I open a list of optical services for a cross-domain link?” (p. 33).

1.24 What is microwave awareness (MWA)?

In networks where multiple Wavence UBT-SA devices are linked to a single 7250 IXR or 7705 SAR NE, the NSP provides microwave awareness. To facilitate network monitoring, MWA shows the router and its linked UBTs, including CA (Carrier Aggregated) UBTs, as a single logical site in Network Supervision, with the following display features:

- The Topology View and Matrix View show the NE and its linked UBT-SAs as a single router NE; the UBT-SAs are not displayed.
- KPIs, and current and historical alarms on UBT-SAs are propagated to the linked router.
- The Equipment Inventory view shows the UBT-SAs as child objects of the router, under Radio Equipment.
- You can cross-launch to the external EMS for UBT-SA devices by right-clicking on their object in the Equipment Inventory view.
- You can search for a UBT-SA object using the object name or IP address.

See the *NSP User Guide* for more information about MWA.

1.25 What is Auto Refreshing?

Network Supervision automatically refreshes KPI and status information at a user-configurable time interval (the Polling Time). You can pause the Auto Refreshing function using the slider in the Utility Drawer at the bottom of the display. This is useful when you want to investigate an issue without the

data changing as you do. When Auto Refreshing is paused, the slider turns red and indicates “Paused”. The date and time of the most recent refresh is always shown.

When Auto Refreshing is enabled, the following are automatically updated after each refresh interval:

- Link status and NE status in the Topology View and Multi-Layer View
- KPIs and other indicators in the Matrix View, Watch Drawer, and Group Access Drawer
- Object status in the Equipment Inventory
- Recent alarms in the Utility Drawer

You can set the refresh interval, or Polling Time, under User Preferences in NSP Settings, available from the **User:** drop-down menu on the NSP Launchpad.

You can manually refresh the display in some views by clicking **Refresh** when it’s available.

1.26 How do I configure application preferences?

You can specify whether an object’s administrative state is used to calculate its KPI level in Network Supervision.

1

Login to NSP as an administrator and launch Network Supervision.

2

In the Network Supervision application, click **More**, **Application Preferences**.

3

Enable or disable the checkbox to use object administrative state for KPI calculations.

4

Save your changes.

END OF STEPS

1.27 How do I configure KPI threshold settings?

Use the KPI Threshold Settings form to specify the affected NE/component counts at which Network Supervision GUI objects change color to indicate status change.

1

In the Network Supervision application, click **More**, **KPI Threshold Settings**.

2

In the KPI Threshold Settings form, drag the cursors on the threshold line to the levels at which you want object color changes to occur.

3

Save your changes.

End of steps

1.28 How do I configure Event Timeline settings?

Note: You must be logged into NSP as an administrative user to complete this procedure.

Use the Event Timeline settings form to enable/disable event logging and specify the object types that appear in the Event Timeline.

1

In the Network Supervision application, click ⋮ **More**, **Timeline Settings**.

2

In the Timeline Settings form, enable or disable event recording in the Network Supervision application.

3

Enable the checkbox for each network object type that you want to appear in the Event Timeline.

4

Save your changes.

End of steps

1.29 How do I configure user preferences?

You can specify a variety of custom view settings in Network Supervision to suit your needs.

1

In the Network Supervision application, click ⋮ **More**, **User Preferences**.

2

In the User Preferences form, configure view capacity, sorting, and refresh settings, as required.

3

Save your changes.

End of steps

1.30 How do I set Utilization Map preferences?

Note: Utilization preferences apply in the session in which they are configured, and in subsequent sessions.

1

In the Network Supervision application, click ⋮ **More**, **Utilization Map Preferences**.

2

Configure the Refresh Rate, Port Speed Settings, and Color settings as required.

Alternatively, restore the default settings.

The Port Speed settings define the thresholds at which the link lines change thickness. The Color settings define the thresholds at which the arrows change color.

3

Close the form.

END OF STEPS

1.31 How do I open an SSH or Telnet session with an NE?

You can use Network Supervision to open an SSH or Telnet session with NEs that are managed using the NFM-P or MDM. The session opens in a browser window.

You can open an NE session from menus in the following locations in the Network Supervision GUI:

- NE tiles in the Matrix View
- The information panel for a selected NE on the Topology View map and Troubleshooting map (in both the Operational and Utilization views), and the Multi-Layer View map
- NEs in the NE List
- NEs in the Watch View
- Alarms in the Current alarms list

There is typically a brief delay before the **Open NE Session** menu item becomes active.

Note: Opening an NE session requires that your user privileges include execute permission for the selected NE. See the User Manager Application Help and your network administrator for more information.

1

Perform one of the following:

a. To open a session from the Matrix View: On the NE tile, click ⋮ **Show More**, **Open NE Session**.

b. To open a session from the Topology View, Troubleshooting Map, or Multi-Layer View: Click

on the NE in the map, then click **Info** to open the Information panel. Click **More actions** , **Open NE Session**.

c. To open a session from the Link List: Hover on an NE in the list and click **More**, **Open NE Session**.

d. To open a session from the Current alarms list: Hover on an alarm in the list and click **More**, **Open NE Session**.

e. To open a session from the Watch View: Hover on an NE in the view and click **More**, **Open NE Session**.

An NE session form opens in a new tab.

2

Select the type of session in the drop-down menu, if required, and click **CONNECT**. NEs that are managed using MDM only use the session type configured in the CLI mediation policy. For SSH sessions with NEs managed using the NFM-P, a Login window appears.

3

Enter the username and password for the NE in the Login window for an SSH session, or in the terminal window for a Telnet session.

4

Click **DISCONNECT** when your session is finished to log out and close the session.

Note: You can click **CONNECT** to open the session again, or enter an IP address in the IP field and click **CONNECT** to open another session with a different NE.

END OF STEPS

1.32 How do I configure physical links?

Note: You must be logged in as an Administrative user to configure physical links.

1

Click **More**, **Physical Links** to open a list of manually-created physical links in the Topology View.

2

In the Manually Created Physical Links form, click **Create Physical Link**. In the Create Physical Link form, you specify the Name, Description, Latency, and Media Type for the link.

3

Click **Add Endpoint** to search endpoints for the link.

4

Select Port or Network Element from the menu and then click **Find Port | Network Element**.

Depending on the object you are searching, you can search by system address, name, or port name.

5

When you have finished adding endpoints, click **Create**.

END OF STEPS

1.33 How do I open a list of optical services for a cross-domain link?

Cross-domain links between the IP and optical domains are shown in the Topology View, Multi-Layer View, and Link List. From any of these formats, you can open a list of optical services that use the optical endpoint of the link.

1

To open a list of optical services in the Topology View or Multi-Layer View:

1. Select a cross-domain link on the map. Information about the link is displayed in the Information panel.
2. Hover over the ⋮ **More Actions** button for a link, then select **Show Optical Services**. A list of optical services that terminate on the optical endpoint of the cross-domain link is displayed.
3. View information about the optical services. Filter and sort the list as required.
4. To view the endpoints for an optical service, hover over the service and click **Endpoints**. The endpoints are displayed.

2

To open a list of optical services from the Link List:

1. Hover over a cross-domain link in the Link List, then click ⋮ **More Actions** , **Show Optical Services**. A list of optical services that terminate on the optical endpoint of the cross-domain link is displayed.
2. View information about the optical services. Filter and sort the list as required.
3. To view the endpoints for an optical service, hover over the service and click **Endpoints**. The endpoints are displayed.

END OF STEPS

1.34 How do I filter the Topology View?

You can configure filters in the Topology View to control the display of information and reduce clutter. Both the Operational and Utilization views allow filtering.

1

In the Topology View, click **Add Filter** and select one of the filter types. A chip filter  is added to the map.

In the Operational view, the filter types are Alarm Severity, Chassis Type, Network Type, Product Type, and Status. You can add up to three filters.

In the Utilization view, the filter types are Utilization and Link Capacity.

2

Click on the chip filter and select one or more criteria related to the filter type.

3

Click **Close** on a chip filter to remove it from the map.

END OF STEPS

1.35 How do I highlight links by type in the Topology View?

The Topology view provides an option to highlight selected link types on a map, using colors to identify the type of link. You can highlight the following link types:

- Copper: Ethernet link using coaxial copper cable
- Fiber: Ethernet SFP link using optical fiber cable
- LAG N+0: LAG link without protected ports
- LAG N+N: LAG link with member ports protected (supported for Wavence NEs only)
- Protected: protected radio link (supported for Wavence NEs only)
- Unprotected: unprotected radio link (supported for Wavence NEs only)

1

Choose the Topology View from the Format Changer drop-down.

2

Click **View Options** to open the Link Highlight Options panel.

View options are available in the Operational view of the Topology View.

3

Click on the icons to enable or disable highlighting for each of the link types. The links on the map show colors indicating the link type.

END OF STEPS

1.36 How do I manage clusters in the Topology View?

You can reduce the number and density of NE objects in the Topology View by enabling clustering, which combines NEs into clusters that show as a single icon. Cluster icons are square with rounded corners.

Clustering can be based on either region grouping or proximity.

Region-based clustering is available for supervision groups enabled for Physical Map Layout; see “Physical Map Layout” in the 1.10 “How do I work in the Topology Map?” (p. 12) topic. Clusters are based on the region and zone groupings configured by an administrator, and are not affected by proximity or zoom level. Typically, region-based clusters and the objects they contain are positioned on a background map according to their actual geographical location.

Proximity-based clustering is available for all supervision groups. Proximity refers to the separation of object icons on the map display. As you zoom in, the cluster icons automatically open to show the NE icons they contain, and when you zoom out, NEs that are close together are automatically clustered, according to cluster range and limit settings.

1

On the map controls panel, click **Adjust clustering** . The Clustering controls menu opens. Configure the following, as required:

- **Cluster by regions**. Enables or disables region-based clustering. Region-based clustering is available only for supervision groups enabled with Physical Map Layout.
- **Cluster by proximity**. Enables or disables proximity-based clustering. Available only when the **Cluster by regions** slider is disabled. Proximity-based clustering is supported for all supervision groups.
- **Show cluster health**. Enables or disables status indicators on cluster icons. NE status is indicated by the inner circle in the cluster icon. Link status is shown as a ring around that circle. You can choose a pie chart or a solid color format. The indicators show the color for the most severe status for NEs and links in the cluster. Pie charts show the percentage of NEs and links with the most-severe status (but for very small percentages, a minimum of 12% is displayed for visibility). From most to least severe, the order for NE (vertex) status is Failure, Unreachable, Resyncing, Maintenance, Unknown, Normal; and for link status: Failure, Maintenance, Unknown, Normal. See the Legend for vertex and link status colors.
- **Show boundaries**. Enables or disables the grey boundary area that appears when a region-based cluster is opened. Available only when the **Cluster by regions** slider is enabled.
- **Cluster inclusion range**. For proximity-based clustering, sets the separation distance at which NEs are clustered, subject to the zoom level.
- **Cluster limit – Network**. For proximity-based clustering, allows clustering of densely located NEs in addition to clustering based on the cluster inclusion range, so you can cluster groups of NEs even if the cluster inclusion range setting doesn’t. This network-wide setting applies to all supervision groups.
- **Cluster limit – Screen**. For proximity-based clustering, allows clustering of densely located NEs in addition to clustering based on the cluster inclusion range, so you can cluster groups of NEs even if the cluster inclusion range setting doesn’t. This screen-based setting applies to the current supervision group, screen view, and zoom level. You can preserve the view and layout by clicking **More** , **Save as My Layout**.

- **Moving a zone or region icon also moves its contents**. When enabled, if you change the placement of a region-based cluster, any zones and NEs within that cluster will also move to the new location on the map. When disabled, you can change the placement of a region-based cluster, but any zones and NEs within that cluster will retain their original map locations when the cluster is opened. Available only when the **Cluster by regions** slider is enabled.
- **Group NEs that are outside the current zone or region**. When you open a region or zone to see its members (the zone, subzone, or NE icons), some of those icons may show connectors to NEs in other regions. You can control the level of detail for connectors to those "outside" NEs using the options under **Group NEs that are outside the current zone or region**. For more detail, choose the **With immediate parent** option; the map displays all connectors to zones or subzones that immediately contain the connected NEs. For less detail, choose the **With top region** option to show a single connector to the region icon. You can navigate to the regions or immediate parent zones by double-clicking on their connector icons.

2

To open the contents of a proximity-based cluster on the map, double-click on the cluster icon, or zoom in. Zoom out to restore clusters.

3

To open the contents of a region-based cluster on the map, double-click on the cluster icon. To back out to a higher cluster level, use the Map Layout Regions navigation path above the map. Zoom controls do not open or restore region-based clusters.

Note: You cannot open region or zone icons while in the Utilization map view. Switch to the Operational view for full navigation of region-based clusters.

When a region or zone contains zones or subzones, the map shows a stacked cluster icon. Click **Legend**, **Clusters and Bundles** for more information.

Whether they are clustered or not, when objects share the same physical location, the map shows a stacked icon shaded blue. Click **Legend**, **Vertex Types** for more information. To see the co-located objects individually, drag them off the stack.

It can happen that one or more NEs in a supervision group are not assigned to any region. In such a case, the topology map creates a cluster called "Nodes without a region" that contains the unassigned NEs. Double-click to access the NEs in the "Nodes without a region" cluster, and contact an administrator if required. NEs can only be assigned to regions by an administrator using the Group Manager application.

END OF STEPS

1.37 How do I save and restore layout changes in the Topology View?

In the Topology View, you can click and drag map objects to change their placement on the map layout. Perform this procedure to save a new layout, or restore the map to the common layout set by an administrator.

1

Click and drag map objects to place them according to your needs. You can drag NEs, links, or clusters.

Note: If the supervision group is enabled for Physical Map Layout, when you move a cluster object the contents of that cluster may keep their original locations, depending on clustering control settings. See 1.36 “How do I manage clusters in the Topology View? ” (p. 35).

2

To save the new layout for the current and subsequent sessions, click ⋮ **More**, **Save as My Layout**.

3

To return the map layout to the common layout set by an administrative user, click ⋮ **More**, **Restore to Common Layout**.

4

To set the current map layout as the common layout, click ⋮ **More**, **Set as Common Layout**. This option is available only for supervision groups that are not enabled with Physical Map Layout. You must have administrator permissions to perform this step.

For supervision groups enabled with Physical Map Layout, administrators must use the Group Manager application to save a common layout; see the Group Manager Help.

END OF STEPS

1.38 How do I find NEs in the Topology View?

Use this procedure to find specific NEs in the Topology View.

1

Click ⌖ **Find in Map**.

2

Select an object type from the drop-down menu. You can search for NEs by name or management address.

3

Type a search string in the text field. A list populates with potential matches as you type.

The list displays a maximum of fifty results. If the NE you are trying to find is not in the list, refine your search string.

4

Click on an item in the list to find that NE in the map.

End of steps

1.39 How do I create views and supervision groups?

You create network views and supervision groups for Network Supervision using the Group Manager application.

You can open Group Manager from the Network Supervision GUI:

1. In the upper right-hand corner, click ⋮ **More**, **Group Manager**.
2. See the Group Manager application help for information on creating network views and supervision groups.

1.40 Mediation software capabilities

Actions performed on objects in the Network Supervision application depend on the capabilities of the object's source mediation software. In particular, certain application functions described in the Network Supervision Help may not be available when the NSP is deployed with the NFM-T, but in the absence of the NFM-P:

- The Event Timeline function is disabled for NFM-T objects in the Watch view, NE Matrix, and NE list.
- Event Timeline settings cannot be configured in an NFM-T-only deployment. Default settings are used.
- The Policy Agent function is not available in an NFM-T-only only deployment.
- The CBAM Access Point function is not available in an NFM-T-only deployment.

1.41 MDM adaptors and Network Supervision

Available application functions for model-driven NEs in Network Supervision can vary based on the adaptors installed. To verify the adaptors you have installed, check the Discovered NEs list in the Device Administrator application. The Summary panel for the NE provides the list of adaptors installed for each application.

1.42 Map view performance

Users should consider the performance information in this section when working in Network Supervision map views.

Nokia recommends a maximum of 2000 NEs per supervision group. Multi-layer maps support a recommended maximum of 4000 objects.

Users should expect the following Multi-layer map loading times with different numbers of NEs:

- for 250 NEs (125 physical links); approximately six seconds for the initial page loading and four seconds to reload

- for 500 NEs (250 physical links); approximately nine seconds for the initial page loading and six seconds to reload
- for 2000 NEs (1000 physical links); approximately 50 seconds for the initial page loading and 28 seconds to reload

1.43 How do I purge assurance event records?

The Event Timeline in applications is a log of events that is mapped over a specified period of time. You can filter the event types presented on the timeline, such as alarm events, OAM test failures, and configuration and state change events. You can use the Event Timeline to search for patterns in events over a period of time.

Perform this procedure to purge assurance event records when the AssuranceEventLoggingTurnedOff alarm is raised. This alarm is raised when the database disk space used to log assurance events grows above the predefined threshold.

Assurance Event logging is disabled to protect the database disk space.

Note: You must be logged into the NFM-P as an administrator to perform this procedure.

1

From the NFM-P main menu, choose Tools→Events→Event Policies. The Manage Event Policies form opens.

2

Choose the assurance.AssuranceEvent event type and click Properties. The Event Policy - assurance.AssuranceEvent (Edit) form opens.

3

Click the More Actions button and choose Purge Event Records. The Event Policy - assurance.AssuranceEvent (Edit) Filter form opens.

4

Click OK to purge all event records.

5

If necessary, configure the Event Retention Time (hours) to a value lower than the default value.

6

Save the changes and close the forms.

END OF STEPS

1.44 NFV API support

For general information about developer support, see the API documentation page on the Network Developer Portal

Before you can perform NFV functions using the REST API, an administrator must enable the NFV Server application. See the *NSP System Administrator Guide* for information about enabling applications. Documentation for the NFV API can be found at:

https://*nsp-server-ip*:8543/NfvServer/api-docs/

The NFV Server application is required to perform the following NFV functions using REST:

- VNF object management (for example, scale-in)
- CBAM access point management
- KPI policy management

Note: Logs for the NFV REST server can be found in the following location on the NFM-P server:

`/nfmp/server/nms/web/tomcat/logs/NfvServer.log`

Note: When performing a Create KPI Policy, Update KPI Policy, or Associate VNF to Policy request using REST, ensure that the Name parameter is correctly supplied in the REST request. An invalid name causes the request to fail.

Valid values for the overloadThreshold, underloadThreshold, and healThreshold parameters in the body of a Create or Update KPI Policy vary depending on the policy template.

2 Managing VNFs using CBAM

2.1 What is network function virtualization?

Network function virtualization (NFV) allows network administrators to uncouple network functions from underlay hardware NEs so that the functions can run as software images. These network functions include load balancers, firewalls, and NAT. The purpose of NFV is to provide a simpler way to deliver and manage the network components required for a virtualized infrastructure. Network administrators are able to dynamically deploy network elements and services without needing to physically provision the underlying routers. The virtualized network element that represents the physical NE is called a virtualized network function (VNF).

VNF management is provided by the external application CBAM, to which the NFM-P provides an interface using the Network Supervision application.

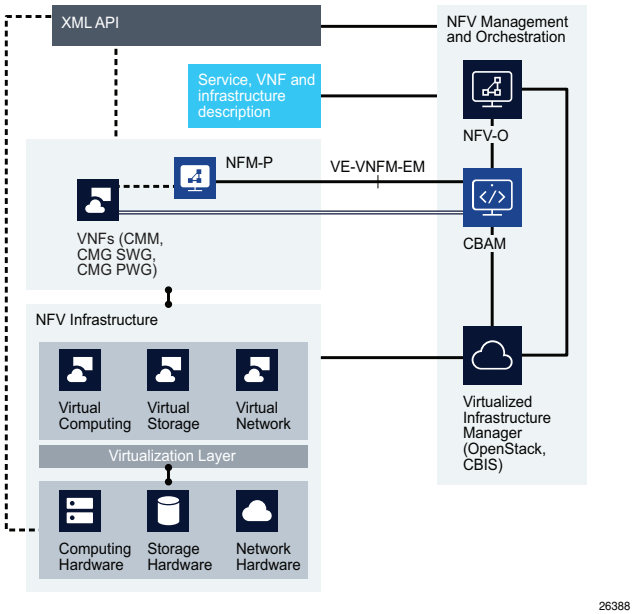
2.2 What is the CloudBand Application Manager?

The Nokia CloudBand Application Manager (CBAM) is a VNF manager that automates VNF lifecycle management and cloud resource management. CBAM has standards-based APIs to allow it to work with any vendor VNF, EMS, VIM, or NFV Orchestrator (NFVO).

The NFM-P provides an interface with CBAM, which acts as the VNF manager in this solution. The NFMP uses the Ve-Vnfm-Em reference point to exchange notifications on VNF lifecycle changes and monitor virtual resources with CBAM. The Network Supervision application allows you to configure a CBAM access point to monitor managed VNFs and execute lifecycle management actions.

The NFM-P provides the following functions when interfacing with CBAM:

- element management for VNFs
- VNF assurance, alarm monitoring, and status tracking
- VNF KPI monitoring
- lifecycle management proxy actions
- policy-based lifecycle changes
- initiating VNF custom actions



2.2.1 Supported VNFs

The CBAM as VNF manager solution currently supports the following VNFs:

- CMG
- CMM
- VSR-I
- CSGN

2.3 What is a CBAM access point?

The NFM-P supports CBAM integration through a CBAM access point created in the Network Supervision application. You must input CBAM and NFM-P login credentials in order to create the access point. You must also specify NFM-P discovery rules to enable VNF automatic discovery. This procedure requires administrator or nfvMgmt access privileges.

Once the access point is successfully created, you can view a list of CBAM access points associated with the NFM-P. From the list of CBAM access points, you can cross-launch to the CBAM GUI, re-scan CBAM VNFs, or open the Details tab for an access point. The Details tab allows you to view the associated discovery rule and the connection status for the specified CBAM access point. The connection status is also displayed in the list of CBAM access points, and is

verified by the NFM-P once every two minutes. If the NFM-P fails to connect to a CBAM access point three times in a row, the access point is marked as disconnected and an alarm is raised.

The following are prerequisites before creating a CBAM access point:

- Ensure the specified CBAM login credentials have access to the CBAM APIs via ReST. See the *Installing CloudBand Application Manager Guide* for more information.
- Ensure the NFM-P SSL certificates are installed on CBAM. See the *CloudBand Application Manager Administrator Guide* for more information.
- If the CBAM access point uses an IPv6 address, ensure the CBAM can resolve the address or hostname of the NFM-P server.

2.3.1 Reconnecting a CBAM access point

When the connection to a CBAM access point is interrupted, you can trigger a manual connection attempt using the Network Supervision application. In the CBAM Access Points list, click on the access point you need to reconnect, and click the Retry Subscription icon.

The NFM-P verifies the connection to a CBAM access point once every two minutes. If the connection attempt fails three times in a row, the NFM-P raises an alarm and stops attempting to verify the connection, instead marking the access point as disconnected.

2.3.2 VNF fault management

The NSP supports receiving alarms based on CBAM fault notifications. Alarms received through a CBAM access point appear in the Network Supervision and Fault Management applications.

The following prerequisites are required in order to receive alarms from a CBAM access point:

- CBAM Release 19.5 SP1 or later
- vnf_resource_fm must be enabled through the CBAM CLI, using the following command:
  `sudo ectl—set /cbam/cluster/services/vnf_resource_fm enabled`
- The CBAM client user for the NSP must have the ve-vnfm-em_zone role enabled.

2.4 How do I integrate a CBAM?

Before you can perform manual and automatic lifecycle management tasks through the Network Supervision application, you must configure a CBAM access point.

Once the access point is successfully created, you can view a list of CBAM access points associated with the NFM-P. From the list of CBAM access points, you can cross-launch to the CBAM GUI, rescan CBAM NFVs, or open the Details tab for an access point. The Details tab allows you to view the associated discovery rules and the connection status for the specified CBAM access point. The connection status is verified by the NFM-P once every two minutes. If the NFM-P fails to connect to a CBAM access point three times in a row, the access point is marked as disconnected and an alarm is raised.

Note: If you are using the NSP in shared-mode deployment, ensure that the auth_nfmp_ enabled parameter in the NSP is set to true so that NFM-P users are authenticated; see the NSP documentation for more information about configuring user authentication.

Note: NAT is supported in standalone and redundant NFM-P deployments (NFM-P clients use hostname). When CBAM is in another subnet, the /etc/hosts of CBAM must be populated with the public IPs and hostnames of both NFM-P instances in case of redundant deployment. The NAT present between the CBAM and NFM-P does the address translation.

2.4.1 Workflow to create a CBAM access point

The following workflow describes the steps to create a CBAM access point.

1. If required, create an NFM-P user account assigned to a user group with the NFV Operator role. See the *NFM-P Administrator Guide* for information about creating users.
2. If required, create discovery rules in the NFM-P for the VNFs you need to discover. See the *NSP NFM-P User Guide* for information about creating discovery rules.
3. Ensure the specified CBAM login credentials have access to the CBAM APIs via ReST. See the *Installing CloudBand Application Manager Guide* for more information.
4. Ensure the NFM-P SSL certificates are installed on CBAM. See the *CloudBand Application Manager Administrator Guide* for more information.
5. Ensure the CBAM is configured for alarm subscription. See 2.3.2 “VNF fault management” (p. 43).
6. If the CBAM access point uses an IPv6 address, ensure the CBAM can resolve the address or hostname of the NFM-P server.
7. Using the Network Supervision application, create a CBAM access point. See 2.5 “How do I create a CBAM access point?” (p. 43).

2.5 How do I create a CBAM access point?

Before you can perform manual and automatic lifecycle management tasks on CBAM-managed VNFs through the Network Supervision application, you must configure a CBAM access point. See Chapter 2, “Managing VNFs using CBAM”.

2.5.1 To create a CBAM access point

1

In the Network Supervision application, click on the More button and select CBAM Access Points. The CBAM Access Points list appears.

2

Click on the Add button. The Add CBAM Access Point panel appears.

3

Configure the parameters. For the NFM-P user name and password, provide the credentials of a user account assigned to a user group with the NFV Operator role.

Note: The user account you provide must not be assigned to a user group with the Administrator role.

4

Perform the following for each VNF product type you need to discover:

1. Click on the + button beside Add VNF Product Types. A VNF product type row is added to the form.
2. Configure the VNF Type parameter. VNF product names associated with the chosen VNF type appear in the VNF Product Names field. If required, click on the Edit button beside the VNF Product Names field and enter additional custom VNF product names.
3. Select discovery rules for the VNF type. You can select a discovery rule for each VNF component of a compound NE, and separate discovery rules for IPv4 and IPv6.

5

To use the CBAM API v4.0 for this access point, enable the Use API v4.0 parameter.

6

Click on the Add button. The CBAM access point appears in the CBAM Access Points list.

END OF STEPS

2.6 How do I discover a CBAM as a GNE?

You can discover a CBAM server as a GNE using the NFM-P to perform basic equipment and alarm management. This section provides information specific to CBAM server configuration and discovery in the NFM-P. The *NSP NFM-P User Guide* chapter "Device commissioning and management" and the *CloudBand Application Manager Administrator Guid*e section “CBAM management over SNMP interface” should be consulted for full procedural details.

2.6.1 Alarm management support

The following table describes NFM-P alarm management support limitations for the specified CBAM releases. For a list of CBAM alarms, see the CBAM alarm documentation.

CBAM Release	Notes
18.5	SNMPv2 mediation only.
19.0	A limitation in the CBAM can create a discrepancy between alarms displayed in the CBAM GUI and the NFM-P. You can compare against the alarm list in the CBAM GUI and use the NFM-P to clear stale alarms.

19.5 MP4	CBAM 19.5 MP4 supports two modes of operation for the SNMP interfaces for Fault Management (FM) and Performance Management (PM): 1. FM and PM on the same port, with a common credential set. SNMPD acts as an SNMP proxy, and the port is fixed to 161. 2. FM and PM on separate configurable ports, with separate credential sets To configure a CBAM as GNE in NFM-P using SNMPv3 management, mode two is required. The default port for the SNMP interface is set to 32161 (which is reconfigurable with values between 10000-65535). On the NFM-P side, the permitted ports for SNMP mediation are: 32161 and 30105. For SNMPv2 management, either mode can be used. See the CBAM Application Manager Administrator Guide for information about SNMP configuration.

2.6.2 Post-installation instructions

The following instructions provide information specific to CBAM server configuration and discovery in the NFM-P. Perform the following

1. Use the NFM-P client to create an SNMP v2 mediation policy for CBAM management. See the *NSP NFM-P User Guide* for information about creating mediation policies.
2. Use the NFM-P to configure a discovery rule for the CloudBand Application Manager that includes the SNMP v2 mediation policy; see the *NSP NFM-P User Guide* for information about creating discovery rules.

2.7 How do I upgrade a CBAM access point?

After you upgrade the software on a CBAM access point, the Network Supervision application attempts to establish communication with the access point. The following table describes post-upgrade tasks that may be required when you upgrade a CBAM access point.

Task	Steps
Enable CBAM API v4.0 support	Enable the Use API v4.0 parameter on the CBAM access point configuration form in the Network Supervision application.

2.8 VNF discovery

You cannot instantiate VNFs using a CBAM interface. You can only discover VNFs from CBAM using NFM-P discovery rules specified during access point creation. The NFM-P requires that the VNFD template for discovered VNFs have post-instantiation scripts to enable SNMP and configure other protocols necessary for automatic NE discovery. When the NFM-P discovers VNFs from a CBAM access point, it adds them as a rule element for the associated discovery rule.

The Unmanaged VNFs tab lists the VNFs managed by the CBAM instance that were not discovered by the specified NFM-P discovery rule. The list is updated once every two minutes.

2.9 How do I instantiate a VNF?

You can instantiate a VNF in the Uninstantiated VNFs tab of the CBAM Access Point form. Before you can instantiate a VNF, you require a JSON file for the VNF, which can be stored locally.

1

In the Network Supervision application, click on the More button and select CBAM Access Points. The CBAM Access Points list appears.

2

Choose a CBAM access point and click on Details. The CBAM Access Point form appears.

3

Click on the Uninstantiated VNFs tab. A list of uninstantiated VNFs appears.

4

Choose a VNF and click on Instantiate. The Instantiate form appears.

5

Click Choose File and provide the JSON file for the VNF to be instantiated.

6

Click on the Instantiate button. The VNF is instantiated, and the instantation event is added to the Event Timeline.

END OF STEPS

2.10 How do I upgrade a CMG?

You can trigger an upgrade of a CMG VNF managed by the CBAM using the Network Supervision application. Before you can trigger the upgrade, the following two files are required:

- A CMG upgrade package, which must be uploaded to the CBAM catalog. See the CBAM documentation for more information about using the catalog.
- A CMG upgrade JSON file, which can be stored locally.

1

Select a CMG and click on the More button, then select Upgrade. The upgrade panel opens.

2

Specify the package ID for the upgrade package in the Package Version parameter. You can obtain the package ID from the catalog on the CBAM.

3

Click on the Choose File button, and select the upgrade JSON file that corresponds to the upgrade package.

4

Click Upgrade, then click OK to confirm. The CMG is placed in an Upgrade state in the Network Supervision application until the upgrade is complete.

End of steps

2.11 What are lifecycle change notifications?

Lifecycle change notifications (LCNs) are messages sent from CBAM to the NFM-P with details on VNF lifecycle updates. When the CBAM access point is created, the NFM-P requests two different LCN subscriptions for the CMG and CMM. LCNs are used to inform the NFM-P of changes related to VNF instantiation, termination, scaling, healing, or variable modifications. When the NFM-P receives an LCN, it scans the VNF information from the CBAM access point and updates its VNF database accordingly.

Regardless of LCNs, the NFM-P automatically polls the CBAM access point for VNF updates once every hour.

Note: In a redundant deployment scenario, the CBAM LCN subscription fails after main server switchover takes place. To re-subscribe, you must restart the Network Supervision application and open the CBAM access point.

2.12 What is VNF lifecycle management?

Certain VNF lifecycle changes can be initiated from CBAM or the Network Supervision application. Whenever a lifecycle change is triggered in CBAM, it informs the NFM-P via an LCN.

VNFs can be instantiated in CBAM and advertised to the NFM-P via an LCN. When the NFM-P receives information on a newly instantiated VNF, it creates an associated VNF object and attaches a discovery rule to that object automatically. When the NFM-P discovers a VNF, it retrieves information related to supported operations, scaling and healing templates, extensions, and compute resources.

VNFs can be terminated in CBAM and advertised to the NFM-P via an LCN. When the NFM-P receives information on a terminated VNF, it unmanages the VNF object and removes all associated VNFCs.

VNFs can be deleted in CBAM and advertised to the NFM-P via an LCN. When the NFM-P receives information on a deleted VNF, it removes the VNF from its database and unmanages the associated network element.

VNFs can be healed to trigger a reboot in CBAM or the Network Supervision application. Healing must be enabled in the CBAM VNFD before this operation can be performed in the GUI. If the VNFD requires additional parameters for VNF healing, the parameters are visible in the Network Supervision application.

VNFs can be scaled in or scaled out in CBAM or the Network Supervision application. Scaling must be enabled in the CBAM VNFD before this operation can be performed in the GUI. When performing a scaling operation, you must specify a scaling aspect and a new level. The scaling level cannot exceed the maximum scaling level specified in the CBAM VNFD. If the VNFD requires additional parameters for VNF scaling, the parameters are visible in the Network Supervision application.

Note: For the CMM, only CPPS modules can be scaled.

Note: To add or remove cards on the VNF, you must use the scaling operation. Nokia does not recommend using CLI to add or remove cards.

2.13 How do I trigger a custom action on a VNF?

You can trigger custom actions that have been defined for a VNF using the Network Supervision application. The actions must be defined in a TOSCA template that has been configured on the CBAM.

1

Click on the More button on a VNF panel and select VNF > Custom Actions. The Custom Actions window appears.

2

Select a custom action from the drop-down list and click OK. The custom action is triggered. You can view details about the results of the action in the event timeline for the VNF.

End of steps

2.14 What is a VNF Descriptor?

The VNF Descriptor is a package that describes the configuration of the VNF network. It consists of OpenStack Heat templates which define VNF specifications. This section describes the configuration requirements for the CBAM VNFD to allow the NFM-P to discover and manage CBAM VNFs. The VNFD package must be compatible with the release of the CBAM being used to manage the VNFs.

For more information on CBAM VNFD template creation, see the CBAM documentation suite.

2.14.1 Template requirements

Ensure the CBAM VNFD templates meet the following requirements:

- The template must populate the **`vnfProductName`** parameter. This parameter allows the NFM-P to determine which VNFs it is not currently managing. The value of the parameter must use one of the following valid product names:
  - Cloud VMG
  - Cloud MG
  - Virtualized Service Router - Integrated
  - CMM
  - C-SGN
- The VNF instantiation workflow should include the application startup. This ensures that CBAM sends LCNs to the NFM-P only when the VNF application is up. If the application startup is not included in the VNF instantiation workflow, the discovery of the VNF into the NFM-P will be delayed.
- The Ansible workflow should push initial configuration on the VNF. This configuration entails the prerequisite configuration requirements for a network element to be discovered by the NFM-P. The system interface should be configured based on the value defined in the **`systemIpAddr`** extension. This configuration minimizes the error situation where the actual system interface IPAddress is different from its definition in the extension.
- The VNFC healing workflow, if implemented, should include the additionalParam **`vnfcToHeal`** configured with a resourceId. The template must not us a UUID as the parameter value, as is already in use as an OpenStack term. The VNFD should be VIM agnostic and should use only CBAM-specific information.
- The template must include required parameters that should be pushed to the VNF during deployment. The following parameters should be available to the NFM-P as VNF extensions or VNFC resource metadata:
  - The **`systemIpAddr`** parameter must be available as a VNF extension.
  - Each VNFC Resource must contain slotId information that uniquely identifies the card object. For VNFs that do no support cards, there must be information to uniquely identify the object that the NFM-P creates.
  - The OAM/CPM VNFC must include the mgmtIP. The key for this metadata should be **`nokia_vnf_ipAddr`**. For a CMG, the IP from that vnfcResource will be used for the mgmtIP with a **`nokia_vnf_slotId`** of A.
  - Each CMG aspect defined in the template must include an extension that defines the type of card to which is corresponds. This extension helps the domain make decisions during preScale.