



Network Integrity

**Release 8**  
**NI-Director Operations Console**  
**User Guide**

**July 29, 2013**

The content of this document is subject to change without notice.

**Copyright 2012 - 2013**

Nakina Systems Inc., Nakina Systems, Nakina Integrity Solutions, NI-Guardian, NI-Collector, NI-Controller, NI-Framework, NI-Director, Nakina Operations Console, Nakina Network Troubleshooting Console, Nakina Secure Network Access Client, Nakina Command Broker, Nakina Session Broker, Nakina Network Backup and Restore, Nakina Network Audit & Software Delivery, Nakina Network Commissioning, Nakina Domain Activation, Nakina Adapter SDK and Simply Profitable Networks are all trademarks or registered trademarks of Nakina Systems Inc. All other trademarks are property of their respective owners.

All rights reserved.

# Table of contents

<b>1. Revision history</b>	<b>7</b>
<b>2. Getting started</b>	<b>8</b>
<b>2.1 Log in</b>	<b>8</b>
<b>2.2 Understand the user interface</b>	<b>10</b>
2.2.1 About the display controls.	13
<b>2.3 Use the groups navigation tree</b>	<b>14</b>
2.3.1 Group view	14
2.3.2 Alarm view	15
2.3.3 Actions available in the groups navigation tree	15
<b>2.4 Use the Network Elements table</b>	<b>16</b>
2.4.1 Actions available in the Network Elements table	18
2.4.2 Find network elements	20
2.4.3 Working with data in the table	21
2.4.4 Save the visible table data to a file	24
<b>2.5 Set preferences</b>	<b>25</b>
<b>2.6 View plugin details</b>	<b>30</b>
<b>2.7 Launch Network Integrity framework applications</b>	<b>31</b>
<b>2.8 Log out</b>	<b>31</b>
<b>2.9 Change your password</b>	<b>31</b>
<b>3. Viewing network topology</b>	<b>33</b>
<b>3.1 About the Topology view</b>	<b>33</b>
3.1.1 About NE status at a glance	35
3.1.2 About network topology layers	35
3.1.3 Topology view controls	36
<b>3.2 View topology for an NE group</b>	<b>37</b>
<b>3.3 View topology for a specific layer</b>	<b>37</b>
<b>3.4 Refresh the Topology view</b>	<b>38</b>
<b>3.5 View topology for an NE</b>	<b>38</b>
<b>3.6 Add a background image to the Topology view</b>	<b>38</b>
<b>3.7 Reposition NEs in the Topology view</b>	<b>39</b>
<b>3.8 View NE equipment details</b>	<b>40</b>
<b>3.9 View group details</b>	<b>41</b>
<b>4. Viewing shelf level graphics</b>	<b>42</b>
<b>4.1 About the Network Element View window</b>	<b>42</b>
4.1.1 About slot states	44
4.1.2 About circuit pack states	44

---

4.1.3	Circuit pack and slot state examples . . . . .	45
4.1.4	About the Resource Tree. . . . .	46
4.1.5	About the display controls . . . . .	47
<b>4.2</b>	<b>View shelf, circuit pack, port, and interface details</b> . . . . .	<b>48</b>
<b>4.3</b>	<b>Update inventory in the Network Element View window</b> . . . . .	<b>52</b>
<b>5.</b>	<b>Configuring equipment</b>	<b>53</b>
5.1	View equipment configuration information . . . . .	53
5.2	Modify equipment configuration. . . . .	55
5.3	Refresh equipment configuration information . . . . .	57
<b>6.</b>	<b>Monitoring the network for alarms</b>	<b>58</b>
6.1	Understanding alarm colors and values . . . . .	59
6.2	Assess the overall alarm status of the network . . . . .	60
6.3	Information provided for individual alarms . . . . .	61
6.4	View and manage alarms in the entire network. . . . .	62
6.4.1	Filter alarms in the Manage Network Alarms window . . . . .	66
6.5	View and manage alarms in a group . . . . .	67
6.6	View and manage alarms for one network element . . . . .	71
6.7	Dynamically filter alarm data. . . . .	73
6.8	Search for alarms . . . . .	74
6.9	Turn dynamic alarm notification on or off . . . . .	75
6.10	View and manage circuit pack alarms . . . . .	76
6.11	Acknowledge an active alarm . . . . .	77
6.12	Add comments to an active alarm . . . . .	78
6.13	Manually refresh alarm data . . . . .	78
6.14	Manually resynchronize alarms with the NE . . . . .	79
<b>7.</b>	<b>Viewing historic alarms, TCAs and other events</b>	<b>80</b>
<b>8.</b>	<b>Performing maintenance</b>	<b>84</b>
8.1	Remove resources from service and return them to service. . . . .	85
8.2	Reset NEs, circuit packs, and ports (warm or cold) . . . . .	86
8.3	Test loopbacks on interfaces or ports . . . . .	87
8.4	Manage protection settings. . . . .	89
<b>9.</b>	<b>Monitoring performance</b>	<b>91</b>
9.1	About the PM Viewer . . . . .	91
9.1.1	About current counts and bin counts . . . . .	92
9.1.2	About polling periods and intervals . . . . .	92

---

9.2	Display PM counts .....	93
9.3	Change the appearance of the graphical view .....	97
9.4	Zoom in and out of the graphical view .....	101
9.5	Export graphical or tabular data to a file .....	102
9.6	Refresh performance monitoring data .....	102
<b>10.</b>	<b>Managing interfaces</b>	<b>104</b>
10.1	Define a far-end interface for a near-end interface .....	104
10.2	Clear a far-end interface setting .....	106
<b>11.</b>	<b>Managing Ethernet services</b>	<b>107</b>
11.1	Common Ethernet Services procedures .....	107
11.1.1	Display the Manage Ethernet Services window .....	107
11.1.2	Search for an NE or interface and select it .....	109
11.2	View the details of an ethernet service .....	110
11.3	Create a Dedicated Internet Access (DIA) service .....	111
11.4	Create an E-Line service .....	116
11.5	Create an E-LAN service .....	119
11.6	Create an E-Tree service .....	124
11.7	Activate a pre-provisioned CPE .....	128
11.8	Modify an ethernet service .....	131
<b>12.</b>	<b>Configuring and using Ethernet OAM</b>	<b>133</b>
12.1	How to obtain more information about Ethernet OAM fields .....	133
12.2	Configuring and using link fault management .....	134
12.2.1	Configure link fault management .....	134
12.2.2	View link fault management details .....	135
12.2.3	Clear link fault management state or statistics .....	136
12.3	Configuring and using connectivity fault management .....	138
12.3.1	Configure and use the continuity check protocol .....	138
12.3.2	Determine connectivity using the loopback protocol .....	139
12.3.3	Configure and use the link trace protocol .....	140
12.3.4	View and clear CFM policer information .....	144
12.3.5	View and clear other CFM data .....	146
12.4	Perform an MPLS LDP traceroute test .....	151
<b>13.</b>	<b>Managing SONET cross-connects</b>	<b>153</b>
13.1	View existing SONET cross-connects .....	153
13.2	Create a SONET cross-connect .....	159
13.3	Delete a cross-connect .....	163
13.4	Change the name of a cross-connect .....	163

---

<b>14. Managing links</b>	<b>165</b>
14.1 View links for an NE or group .....	165
14.2 Create a manual topology link between two NEs .....	170
14.3 View manual topology links in the Topology view .....	174
14.4 Delete a manual topology link.....	174
<b>15. Managing VCGs</b>	<b>175</b>
15.1 View VCGs for an NE or group .....	175
15.2 Modify a VCG .....	179
15.3 Delete a VCG.....	181
15.4 Add a VCG.....	181
<b>16. Launching external applications</b>	<b>183</b>
16.1 Use the Applications menu (global).....	183
16.2 Launch applications in the context of an NE (Application Launch plugin) .....	183
16.3 Use custom NE menu items (NE Launch-pad plugin).....	184
<b>17. Issuing TL1 commands</b>	<b>186</b>
17.1 About the TL1 Command and Control plugin .....	186
17.1.1 About the TL1 Commands window .....	187
17.1.2 About polling .....	188
17.1.3 About command responses .....	189
17.2 Issue TL1 commands to NEs, circuit packs, or ports.....	190
<b>18. Viewing outstanding conditions and autonomous messages</b>	<b>197</b>
<b>19. Using a Telnet or SSH session to communicate with an NE</b>	<b>202</b>
19.1 Establish a Telnet or SSH session .....	202
19.2 Change the appearance of a session window.....	204
19.3 Save a Telnet or SSH session to file .....	206
19.4 Send an ASCII file to an NE .....	207
19.5 Edit text strings in a command.....	207
19.6 Finding text.....	209
19.7 Clear a session window screen .....	210
19.8 Clear the scrollback buffer .....	210
19.9 Restore the window to default properties .....	210
19.10 Close the session window upon disconnecting .....	210
19.10.1 Keep session window open upon disconnecting .....	210

<b>20. Transferring files to and from an NE</b>	<b>212</b>
<b>20.1 About the file transfer window . . . . .</b>	<b>212</b>
<b>20.2 Launch the file transfer client . . . . .</b>	<b>213</b>
<b>20.3 Stop a connection attempt . . . . .</b>	<b>213</b>
<b>20.4 Disconnect from a session . . . . .</b>	<b>214</b>
<b>20.5 Manage files . . . . .</b>	<b>214</b>
20.5.1 Sort files . . . . .	214
20.5.2 Move up a folder . . . . .	214
20.5.3 Create a new folder . . . . .	215
20.5.4 Rename a file or folder . . . . .	215
20.5.5 Delete a file or folder . . . . .	216
<b>20.6 Transfer files to the remote site . . . . .</b>	<b>217</b>
20.6.1 Transfer files to the remote site using the Upload command . . . . .	218
20.6.2 Transfer files to the remote site using the upload icon . . . . .	218
20.6.3 Transfer files to the remote server using the option bar . . . . .	218
<b>20.7 Transfer files from the remote site . . . . .</b>	<b>219</b>
20.7.1 Transfer files from the remote site using the Download command . . . . .	219
20.7.2 Transfer files from the remote site using the download icon . . . . .	219
20.7.3 Transfer files from the remote site using the option bar . . . . .	219
<b>20.8 Change transfer configurations . . . . .</b>	<b>220</b>
<b>20.9 Hide or display the log tabs . . . . .</b>	<b>220</b>
20.9.1 Hide the log tabs . . . . .	220
20.9.2 Display the log tabs . . . . .	221
<b>21. Troubleshooting</b>	<b>223</b>
<b>Appendix A: NE icons in the Topology view</b>	<b>224</b>

# 1 Revision history

---

The following table provides a summary of the major changes made to this document for this release. Each new version of this document supersedes all earlier versions until re-issued.

Issue	Description
July 29, 2013	Re-issued for 8.3 with Manage Ethernet Services features.
April 02, 2013	First issue of this document for NI-Director Operations Console (NOC) release 8 or higher unless reissued

## 2 Getting started

---

This section explains how to get started using the NOC. It provides details about how to:

- “[Log in](#)” on page 8
- “[Understand the user interface](#)” on page 10
- “[Use the groups navigation tree](#)” on page 14
- “[Use the Network Elements table](#)” on page 16
- “[Set preferences](#)” on page 25
- “[View plugin details](#)” on page 30
- “[Launch Network Integrity framework applications](#)” on page 31
- “[Log out](#)” on page 31
- “[Change your password](#)” on page 31



**Note:** If a NOC application is not performing as expected for a specific model of network element, always consult the Adapter Notes for the model and version of the NE in question. The Adapter Notes provide important information about the NOC applications that are supported by each adapter and also provide detailed information about any special considerations, restrictions or limitations that may exist in the adapter or the NE it supports.

You must familiarize yourself with the detailed operation of the network element that is supported by the adapter. The information in the Adapter Notes must be made available to the NOC users so they will know what to expect when managing network elements from the NOC. Before raising a support issue against the NOC be sure to check the Adapter Notes to make sure that the adapter and the NE support the task you are trying to perform and that there are no special considerations or implementation issues.

### 2.1 Log in

Use the following procedure to launch the NOC and log into a Network Integrity web server.



**Note:** The amount of time a NOC session can sit idle before a user is automatically logged off is configurable through the Network Integrity Framework. If your session is terminated after a period of inactivity, it is because this feature has been configured for your user ID. Consult your network administrator for more information.

Before performing this procedure, obtain the following information from your network administrator:

- a valid Nakina user ID and password that has been configured by the administrator with the required roles and permissions

- if required, the host name or IP address of the Network Integrity web server to which the NOC will connect and the port number on the Network Integrity web server to which the NOC will connect - default 8012

You only need this information if you want to choose a specific server to log in to. Otherwise, the NOC will automatically attempt to log in to one of the servers that the administrator specified when the NOC was installed.

1. Launch the NOC:
  - a. For Windows, choose **Start > All Programs > Nakina > NI-Director Operations Console > NI-Director Operations Console**. (Alternatively, you can navigate to the folder where the NOC is installed and double-click the **Nakina Open Console.exe** file.)
  - b. For Solaris, navigate to the folder where NOC is installed, open the **bin** folder and double-click on the **run.sh** file, or open a command window and type **./run.sh**.

The system displays the Login screen.

2. If you want to specify a server and port to log into, click the **Option** button and do the following:
  - a. Type the host name of the Network Integrity web server in the **Server** field.
  - b. Type the SSL port number for the connection to the Network Integrity web server in the **Port** field. The default Web tier SSL port is 8012.

If you do not specify a server and port, the NOC will automatically choose one of the servers that the administrator specified when the NOC was installed.

3. In the **Username** and **Password** fields, type your Network Integrity user name and password.

4. Click **Login**.

A login progress window appears. After a few seconds the login security message is displayed.

5. Click **Continue**.

After a brief initialization period, the NOC main window is displayed, which is the main launching point for surveillance, troubleshooting, configuration and performance monitoring activities. The information that is displayed will depend on which plugins have been configured.

The procedures in this guide show the Windows version of the NOC. The Solaris version of the NOC has a slightly different appearance, but the functions and features are the same.



**Note:** When starting the NOC, the time it takes to launch the user interface and display the NE Groups in the navigation tree can vary depending on your network configuration. In some configurations it can take approximately 25 seconds to launch fully.

6. To access the online help, select **Help > Help Contents**.
7. To use the NOC, refer to the other sections in this guide.

## 2.2 Understand the user interface

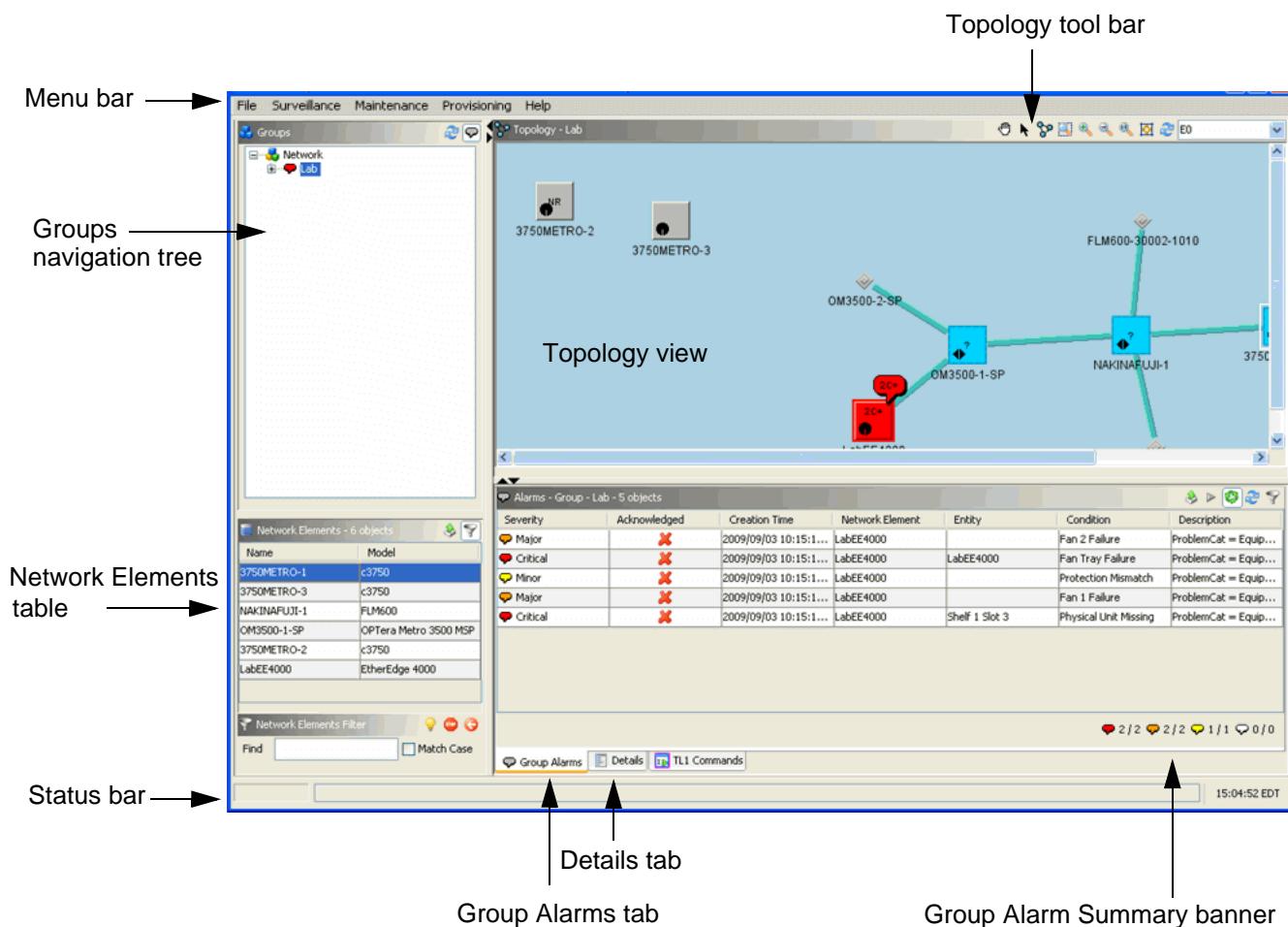
The NOC user interface provides a number of navigational tools, such as a navigation tree and network topology view, menus, and informational areas, to enable you to manage your network efficiently.

This section provides:

- an overview of the features of the NOC user interface, including menu items
- basic procedures for using the navigation tree and Network Elements table to locate and manage NEs.

The following figure shows the NOC user interface and identifies the main features of the interface.

**Figure 2–1: User interface**



"[Features of the user interface](#)" on page 11 describes the NOC user interface features.

**Table 2–1: Features of the user interface**

<b>Feature</b>	<b>Description</b>
Menu bar	See “ <a href="#">Menu bar commands</a> ” on page 12 for descriptions of the items in the menu bar.
NOC application launch-pad (not shown)	The NOC application launch-pad is located directly below the menu bar. It can be configured with clickable icons that provide convenient access to any application that users may require. The NOC application launch-pad is controlled through an XML file called launch_pad.xml, which is configured by your administrator.
Topology tool bar	Contains buttons for controlling the display of the Topology view and a list for selecting the topology layer. See “ <a href="#">Topology view controls</a> ” on page 36 for a description of each of the buttons.
Navigation tree	Displays the NE groups to which your user role has been granted access. For details, see “ <a href="#">Use the groups navigation tree</a> ” on page 14. Selecting a group in the navigation tree automatically changes the information in the Topology view, the alarm view, and the Network Elements table, which display information about the selected group.
Group summary (not shown)	When a container is selected in the navigation tree, a group summary is displayed in the Topology view which shows the highest level of unacknowledged alarm in the group. For details, see “ <a href="#">View and manage alarms in a group</a> ” on page 67.
Network Elements table	Shows the list of NEs contained in the selected group if the group is static or dynamic. The NEs that are displayed are controlled by the Navigation preferences. See “ <a href="#">Set preferences</a> ” on page 25 for more information. You can filter the list by using the Find field. As you type in the Find field, the system dynamically displays the matching NEs. For more information, see “ <a href="#">Use the Network Elements table</a> ” on page 16. By right-clicking on an NE you have access to the tasks that can be performed on it.
Topology view	Shows the icons for the groups or NEs in the selected NE group and draws the topological links for the selected layer. Background images such as maps can be added to the Topology window. For more information about the Topology view, see “ <a href="#">Viewing network topology</a> ” on page 33.
Group Alarms tab	Displays the list of alarms for the selected NE group. For details, see “ <a href="#">View and manage alarms in a group</a> ” on page 67.
Details tab	Displays the attributes of the selected NE. For details, see “ <a href="#">View NE equipment details</a> ” on page 40.
Status bar	Displays NOC process messages.
Group Alarm summary banner	A summary of the current alarm count for the selected group. There are four alarm balloon colors, which represent the severity from highest to lowest (from left to right: Critical, Major, Minor and Warning.) For each severity there is a pair of numbers “x/y”, where x is the number of unacknowledged alarms of that severity in the group, and y is the total number of alarms of that severity in the group.

[“Menu bar commands” on page 12](#) lists the items in the menu bar. The menu bar always contains the File, Maintenance, and Help items, but other items or sub-items may or not be present, depending on the permissions that you have and the plugins that you have installed.

**Table 2–2: Menu bar commands**

Menu	Command	Description
File	Change Password	Open a dialog box that allows you to change your Network Integrity password from the NOC. See <a href="#">“Change your password” on page 31</a> for more information.
	Preferences	Opens a preferences dialog box that contains settings for tooltip display, time zone, and date format. See <a href="#">“Set preferences” on page 25</a> for more information.
	Edit Groups	Opens the NE Group Manager. The system logs you in automatically using the ID and password that you used to log in to the NOC. See the Network Integrity Framework Management Guide or online help for more information about the NE Group Manager.
	Exit	Closes the NOC.
Surveillance	Manage Network Alarms	Open the Manage Network Alarms window, which provides a network-wide view of alarms. See <a href="#">“View and manage alarms in the entire network” on page 62</a> for more information.
Maintenance	Inventory Reports	Opens the Inventory Reports window. The system logs you in automatically using the ID and password that you used to log in to the NOC. See the Network Integrity Framework Management Guide or online help for more information about inventory reports.
	Network Audit	Opens the Network Audit window. The system logs you in automatically using the ID and password that you used to log in to the NOC. See the NI-Director User Guide or online help for more information about network audits.
	Software Delivery	Opens the Software Delivery window. The system logs you in automatically using the ID and password that you used to log in to the NOC. See the NI-Director User Guide or online help for more information about software delivery.
	NE Manager	Opens the NE Manager window. The system logs you in automatically using the ID and password that you used to log in to the NOC. See the Network Integrity Framework Management Guide or online help for more information about NE Manager.

Menu	Command	Description
Provisioning (This menu only appears if the Equipment Configuration, Cross-Connects plugin, the VCG plugin, or the SDC plugin is installed.)	Manage Cross-Connects	Opens the Manage Cross-Connects window. For procedures related to cross-connects, see <a href="#">“Managing SONET cross-connects” on page 153</a> . This menu is only available if the administrator has enabled the permissions for the user’s role and the Cross-Connect Manager plugin has been installed.
	Manage VCG	Opens the VCG Manager, which is used to view and edit virtual concatenation groups (VCGs)
	Launch SONET Domain Manager — Network Element View	These items open the NI-Director SONET Domain Controller (SDC). They are only available if SDC is installed, the administrator has enabled the permissions for the user’s role, and preferences have been set for SDC.
	Launch SONET Domain Manager — Subnetwork Connections Manager	For details about SDC, see the SDC documentation.
Help	Help Contents	Launches the user’s default web browser and displays the online help for the NOC.
	System and Application Properties	Provides information about installed plugins, java properties and memory used.
	About NI-Director Operations Console	Provides information about the NOC software load for the user that is logged in.
Applications	Dependent on configuration	Provides a list of applications that have been configured by your administrator. See <a href="#">“Use the Applications menu (global)” on page 183</a> for more information. If your administrator has not configured any applications, “Applications” is not shown in the menu bar.

## 2.2.1 About the display controls

You can control which sections of the NOC window to hide or display using the display controls provided. The display controls are arrows located between the sections of the main window. The following table explains the function of the controls.

Icon	Use
	Vertical Display Controls — When all frames are displayed, click the left arrow (the top arrow) to hide the left panel. To display it again, click the right arrow (the bottom arrow). When all frames are displayed, click the right arrow to hide the right panel. Click the left arrow to display it again.

Icon	Use
	Horizontal Display Controls — When all frames are displayed, click the up arrow to hide the top panel. To display it again, click the down arrow. When all frames are displayed, click the down arrow to hide the bottom panel. Click the up arrow to display it again.

If you change the display or resize the sections of the window, the changes are saved and the window is displayed the same way the next time you log in to the NOC. Other users of the NOC, whether on the same machine or not, will not see your changes.

## 2.3 Use the groups navigation tree

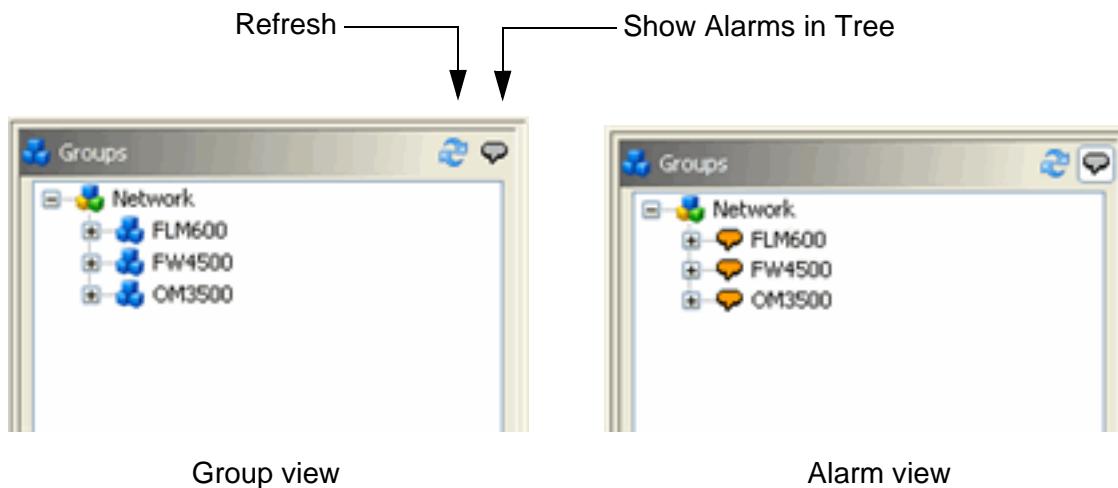
The navigation tree shows the NE groups to which a user has access and also provides alarm indicators for selected NE groups. You have two options for viewing groups:

- group view
- alarm view

See “[Group view](#)” on page 14 and “[Alarm view](#)” on page 15 for details.

To toggle between the two views, click the Show Alarms in Tree icon. The icon is shown in “[Groups navigation tree](#)” on page 14, along with examples of the two views.

**Figure 2–2: Groups navigation tree**



### 2.3.1 Group view

A group is one of the following types:

- static
- dynamic
- container

For details about group types, see the Network Integrity Framework Management Guide or online help.

Static and dynamic NE groups are assigned to a role using the Network Integrity framework. You can see only the NE groups for the role that has been assigned to your user ID.

In the Group view, the top-level Network group contains all the NEs that are managed by Network Integrity. This group cannot be modified or deleted. Clicking on the plus sign (+) beside a container group expands the tree view to display the NE groups it contains. Clicking the minus sign (-) beside a container group collapses the tree view.

Clicking a static or dynamic group displays the NEs in the group in the Network Elements table (see “[Use the Network Elements table](#)” on page 16) and in the Topology window (see “[About the Topology view](#)” on page 33).

### **2.3.2 Alarm view**

In the alarm view, alarm balloons are shown next to the group names. If an alarm condition exists anywhere within a group, the group icon is replaced with an alarm balloon indicating the highest unacknowledged severity. Alarm colors are configurable. For more information about alarms colors and viewing alarms, see “[Understanding alarm colors and values](#)” on page 59.

### **2.3.3 Actions available in the groups navigation tree**

You can perform a number of different actions by right-clicking a group in the groups navigation tree and choosing a menu item, as shown in “[Group context menu](#)” on page 15.

**Figure 2–3: Group context menu**



The menu items that are available are:

- **Expand All** — Expands all groups within the selected group
- **Edit Group** — Opens the NE Group Manager for the group that you chose.

The system logs you in automatically using the ID and password that you used to log in to the NOC.

See the Network Integrity Framework Management Guide or online help for more information about the NE Group Manager.

- Topology — enables you to open the topology for the group in a new window. All topology control apply in the new window. For more information about the topology view, see “[Viewing network topology](#)” on page 33.
- Surveillance — enables you to open a stand-alone list of alarms for the group. See “[Monitoring the network for alarms](#)” on page 58 for more information about alarms.
- Inventory — displays detailed information about the group. See “[View group details](#)” on page 41 for more information.
- Maintenance — enables you to open a command window for the group. See “[Issuing TL1 commands](#)” on page 186 for more information. This option is not available for container groups.
- Provisioning — enables you to manage links or provision Ethernet services. See “[Managing links](#)” on page 165 or “[Managing Ethernet services](#)” on page 107 for more information.

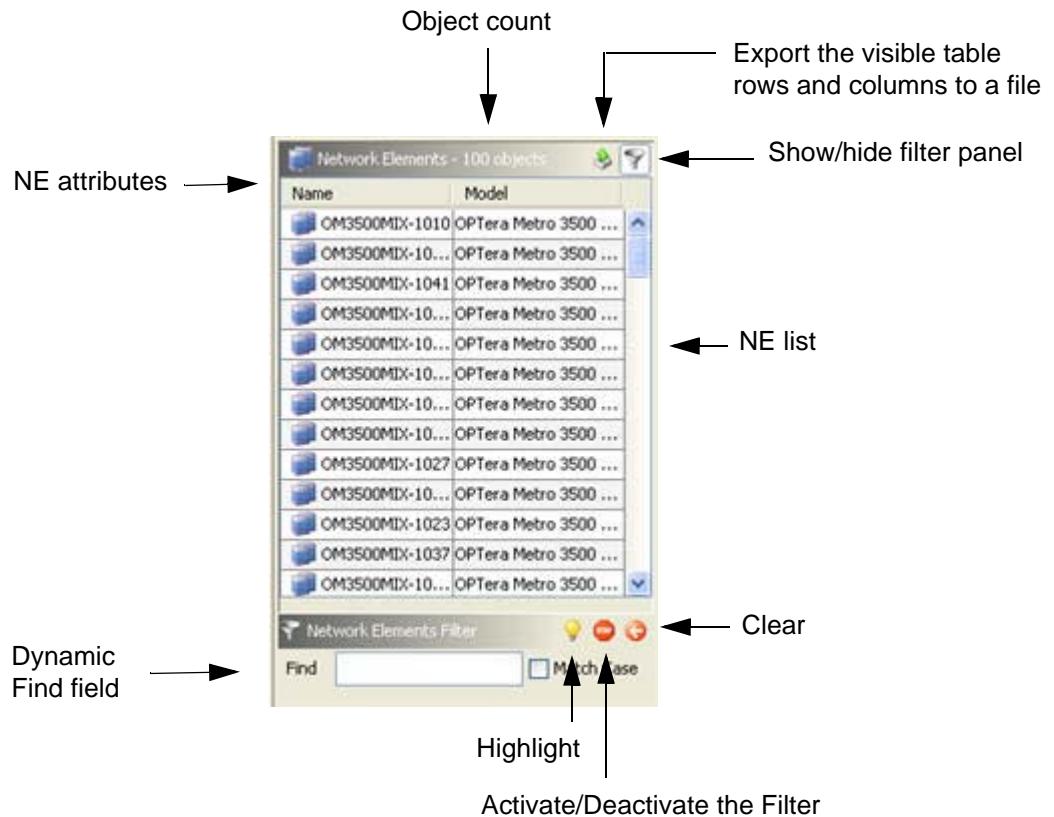


Note: Depending on which plugins you have installed, the sub-menus may differ. For example, if you have installed SDC, additional menu items will be available under the Provisioning menu. These items are described in the sections that explain how to use the plugins or, in the case of SDC, a separate user guide.

## 2.4 Use the Network Elements table

The Network Elements table displays a list of the NEs that are contained in the currently selected NE group.

“[Network Elements table](#)” on page 17 shows an example Network Elements table.

**Figure 2–4: Network Elements table**

The behavior of the Network Elements table can be modified by changes the preferences for loading NE data. For more information see “[Set preferences](#)” on page 25.

The features of the Network Elements table are explained in “[Network Elements table features](#)” on page 17.

**Table 2–3: Network Elements table features**

Feature	Description
NE attributes	The following NE attributes can be displayed: label, vendor, version, model, IP address, type, last updated date.
Object count	Shows the number of NEs in the NE list. When the Highlight button is selected, also shows the number of selected NEs.
Export the visible table rows and columns to a file	Select this button to export the current view of the NE table to a file. For the procedure, see “ <a href="#">Save the visible table data to a file</a> ” on page 24.
Show/hide filter panel	Select this button to control whether the filter panel is displayed.

Feature	Description
NE list	This is the set of NEs in the NE group that is selected in the navigation tree. The search, filter, and sort functions operate on this list. The letter "G" beside the NE icon identifies a gateway NE.
Dynamic Find field	Text that is typed in this field is used to search and filter the NE list. As you type in the Find field, the NE table is dynamically updated with the NEs that match the typed criteria. If the Match Case check box is selected, the case of the text typed in the Find field must match the case of the Label field in the NE list.
Highlight	When this button is selected, the NEs that match the search criteria in the Find field are highlighted in the NE list. All NEs remain displayed in the list. When this button is not selected, the NEs that do not meet the matching criteria are removed from the list.
Activate/Deactivate the Filter	Selecting this button enables or disables filtering of the NE list. When filtering is disabled <ul style="list-style-type: none"> <li>the NE list refreshes to show all NEs in the selected group</li> <li>the Find field and Match Case check box are unavailable, but any data in them is unchanged</li> </ul>
Clear	Clicking this button clears the text in the Find field and, if selected, the Match Case check box. The NE list refreshes to show all NEs in the selected group.

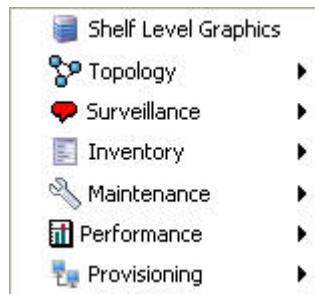
## 2.4.1 Actions available in the Network Elements table

You can perform a number of different actions by right-clicking an NE in the Network Elements table and choosing a menu item, as shown in “[Group context menu](#)” on page 15.



Note: Depending on your permissions and the plug-ins that you have installed, some items may not be available. Contact your system administrator for more information.

**Figure 2–5: Network elements context menu**



The menu items that are available are:

- Shelf Level Graphics — if configured, opens a graphical view of the shelves for the selected NE. For more information about shelf level graphics, see “[Viewing shelf level graphics](#)” on page 42.
- Topology — enables you to open the topology for the NE’s group in the main topology window or in a new window. For more information about the topology view, see “[Viewing network topology](#)” on page 33.
- Surveillance — enables you to open a stand-alone list of alarms for the NE. See “[Monitoring the network for alarms](#)” on page 58 for more information about alarms.
- Inventory — provides the following sub-menu items:
  - Details  
See “[View NE equipment details](#)” on page 40 for more information.
  - View Attributes from Network  
Allows you to obtain NE attributes directly from the NE instead of from the Nakina database and display them in a separate window.
  - NE Credentials  
Provides access to NE credentials. See the Network Integrity Framework Management Guide or online help for details.
  - NE Manager  
Opens the NE Manager. See the Network Integrity Framework Management Guide or online help for details.
  - Inventory  
Opens the Inventory application with the selected NE displayed. See the Network Integrity Framework Management Guide or online help for details.
- Maintenance — provides access to maintenance commands and external applications. For more information about maintenance commands, see “[Performing maintenance](#)” on page 84. For more information about external applications, see “[Launch applications in the context of an NE \(Application Launch plugin\)](#)” on page 183. If the sub-menu items are grayed out, it means that your Network Integrity administrator has not assigned the permission to your user account, or the feature has not been installed.  
Maintenance also provides access to Backup and Restore and NE Request Logs. See the NI-Director User Guide or online help for more information.
- Performance — provides access to collected PMs. The Collected PMs item shows the performance monitoring files that have been collected for the NE and are still in the database. See the NI-Director User Guide or online help for more information.
- Provisioning — enables you to manage links, SONET cross-connects, VCGs, or equipment configuration. See “[Managing links](#)” on page 165, “[Managing SONET cross-connects](#)” on page 153, “[Managing VCGs](#)” on page 175, or “[Configuring equipment](#)” on page 53. for more information.



**Note:** Depending on which plugins you have installed, the sub-menus may differ. For example, if you have installed SDC, additional menu items will be available under the Provisioning menu. These items are described either in the sections that explain how to use the plugins or, in the case of SDC, a separate user guide.

## 2.4.2 Find network elements

Use this procedure to search the current NE list in the Network Elements table. The search criteria operates on all of the visible fields. When you search for an NE, the NEs that meet the search criteria are displayed in the list.

1. Select the group that contains the NE you are searching for.



Note: In order to select and display NEs for the parent “Network” at the top of the navigation tree, you must have the Navigation preference set to “Show Network Elements in Top (Network) Group”. To set preferences, see [“Set preferences” on page 25](#).

2. Type the NE search criteria in the **Find** field and select the **Match Case** option, if required.

If the **Find** field is grayed out, click the **Activate/Deactivate the Filter** icon to enable the field.

As you type, the NEs that match the search criteria are displayed in the Network Elements table.

3. To return to the original NE list, you can do any of the following:

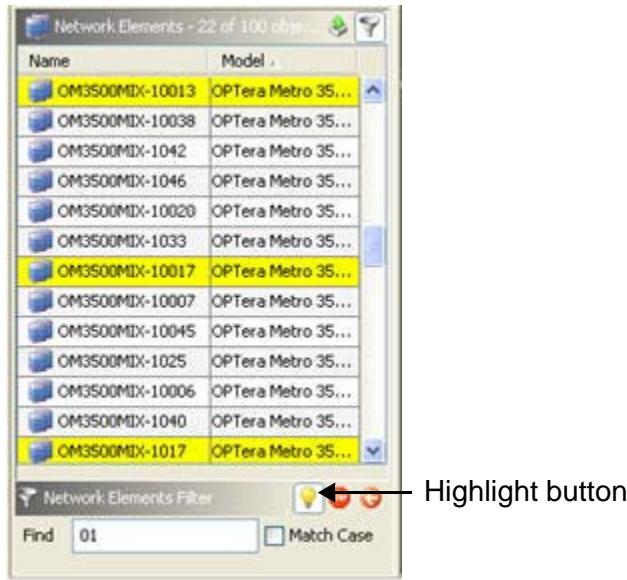
- Delete the text from the Find field.
- Click the **Activate/Deactivate the Filter** button.
- Click the **Clear** button.

### Highlight entries in a filtered table

Use this procedure to highlight entries in the table that match the filter criteria. As the table updates, the items that match the filter criteria are highlighted.

1. Click the Highlight button.

As the list is filtered, items that match the filter criteria will be highlighted in yellow. Highlighting can be turned off by clicking the Highlight button again.



2. To turn highlighting off, click the Highlight button again.

### 2.4.3 Working with data in the table

In the Network Elements table, you can perform a number of tasks to change the appearance or content of the table. Actions that can be performed on tables in the NOC, such as the Network Elements table or the alarms table, are very similar: columns can be sorted, data can be filtered and highlighted, and the displayed data can be exported to a file, plus more.

This section contain the following common procedures:

- “Sort table data” on page 21
- “Add or remove columns in a table” on page 22
- “Rearrange the columns in a table” on page 23
- “Save the visible table data to a file” on page 24

You settings for order and size of the visible columns are saved automatically on a per-user basis. Other users of the NOC, whether on the same machine or not, will not see your changes.

#### Sort table data

Use this procedure to sort the data displayed in a table, such as the list of alarms, either numerically or alphabetically depending on the type of data in the column. Sorting is case insensitive - it does not differentiate between upper-case and lower-case letters.

The columns of the NE table can be sorted in ascending or descending order by clicking on the column heading. An arrow head appears in the column heading indicating which direction the list is sorted. By default sorting is off.

- Clicking once sorts in ascending order.
- Clicking a second time sorts in descending order.
- Clicking a third time turns sorting off again.

Rows are sorted according to the order that the columns are selected. For example, if a user wants to sort on Model first, then Name within Model, the user must first click on the Model header, and then click on the Name header.

To sort on more than one column, Ctrl-click each column heading that you want to sort on. The first column you Ctrl-click on has the highest priority in the sort and the last column you Ctrl-click on has the lowest priority in the sort.

1. Click on the table heading of the criteria that you want to sort by, such as Name. An arrow appears in the Name header and the Name column is sorted in ascending order, as shown in the following example:

Name	Model	OP
OM3500MIX-10001	OF	
OM3500MIX-1001	OF	
OM3500MIX-10010	OF	
OM3500MIX-10011	OF	
OM3500MIX-10012	OF	
OM3500MIX-10013	OF	

2. Click the table header again to reverse the sort order.

The arrow changes direction and the order of the rows is reversed, as shown in the following example:

Name	Model	OP
OM3500MIX-1019	OF	
OM3500MIX-1018	OF	
OM3500MIX-1017	OF	
OM3500MIX-1016	OF	
OM3500MIX-1015	OF	
OM3500MIX-1014	OF	

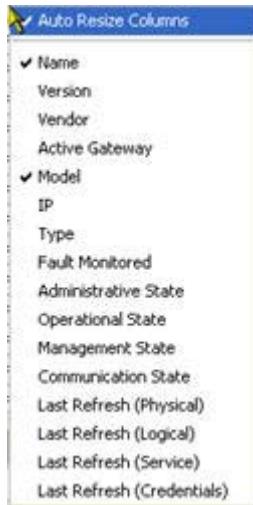
3. Click a third time to cancel the sorting.

### Add or remove columns in a table

Use this procedure to change the columns that are displayed by adding or removing columns to the alarm list. If you are going to export table data to a file, only the information from the displayed columns will be exported.

1. Right click on a column heading and select or deselect the desired column headings to toggle the selection. A check mark indicates that a column will be

displayed. The selections that are available will vary according to the data being displayed.



For example, if you wanted to see, in tabular format, the NEs a group that were out of contact, you could add the “Communication State” column to the Network Elements table and then sort on that column:

Name	Model	Communication ...
FW4100-02-35009-0		Out of Contact
OM3500EVENTS-2045-0	OPTera Metro 3500 MSP	Out of Contact
FW4500CR52-35006-0	Flashwave4500	Out of Contact
FW4500PM-35008-0	Flashwave4500	Out of Contact
OM3500MIX-30001-1...	OPTera Metro 3500 MSP	In Contact
FW45001-30005-1003	Flashwave4500	In Contact
FW4500-30004-1003	Flashwave4500	In Contact
FW45001-30005-1002	Flashwave4500	In Contact
FW4500-30004-1004	Flashwave4500	In Contact
FW45001-30005-1004	Flashwave4500	In Contact
FW45001-30005-1001	Flashwave4500	In Contact
OM3500CIRC-40001-...	OPTera Metro 3500 MSP	In Contact
FW4500-30004-1001	Flashwave4500	In Contact
OM3500EVENTS-3204...	OPTera Metro 3500 MSP	In Contact

2. If you want the columns to be automatically resized as they are added to the table, leave the Auto Resize Columns option enabled.

The option is enabled by default. If you clear it, each column added is an equal width and the columns do not expand to fit the available space.

Your choice for Auto Resize Columns is saved automatically. Other users of the NOC, whether on the same machine or not, will not see your changes.

### Rearrange the columns in a table

Use this procedure to rearrange the columns in a table so that they are in a different order. Columns can be dragged left or right to the position that you want.

1. Left click on a column heading and drag the column to the left or right until it is in the position that you want.

In this example, the user has clicked on the Model heading and is dragging it to the right.

Name	Version	Vendor	Active Ga...	Model	
OM350...	12.1	Nortel		OPTera Met...	ic
OM350...	12.1	Nortel		OPTera Met...	ic

Drag the column left or right

#### 2.4.4 Save the visible table data to a file

Use this procedure to save the currently visible table data to a file. You can save data in a number of different formats:

- PDF — portable document format for viewing with Adobe Acrobat
- RTF — rich text format for viewing or editing in a word processor like Microsoft Word
- HTML — for viewing in a web browser
- CSV — comma-separated value format for opening as a spreadsheet
- XLS — Excel format (single-page) for viewing in Excel or compatible spreadsheet application

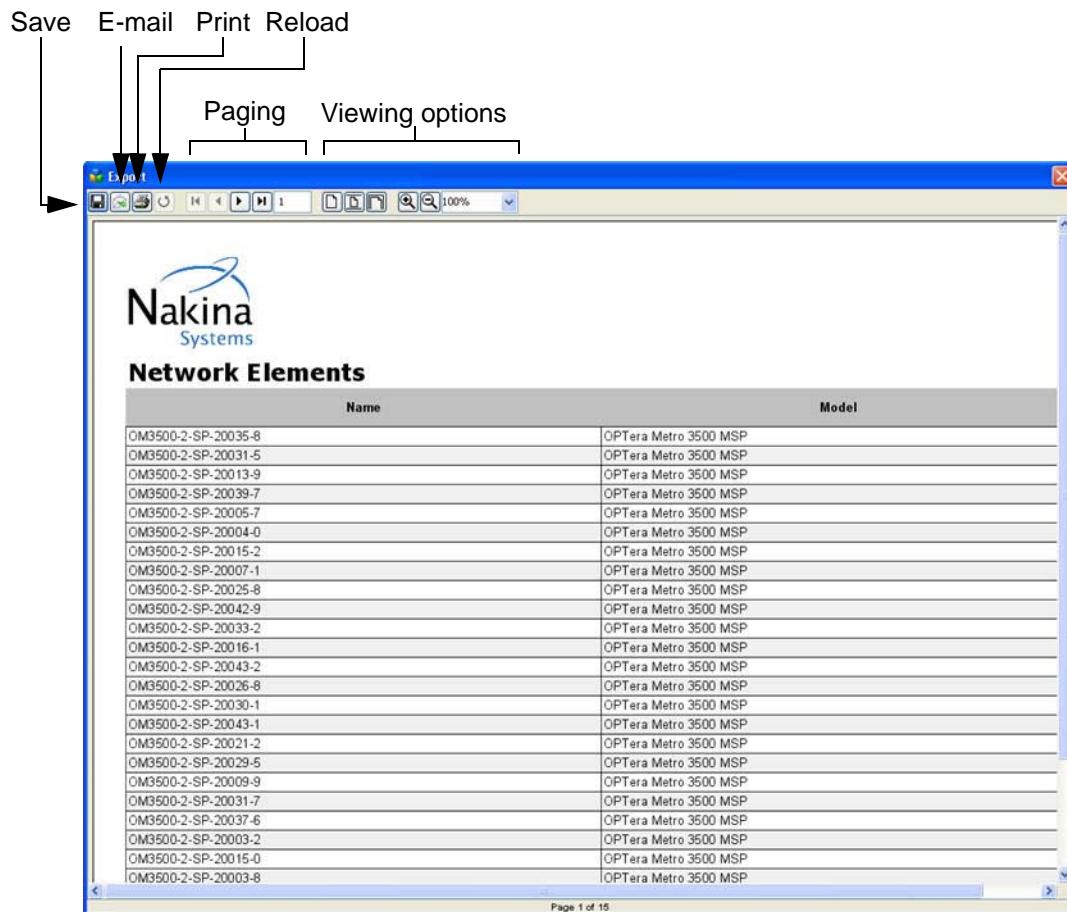
You can also email the file to one or more recipients.

If you want to add or remove data before exporting, see “[Add or remove columns in a table](#)” on page 22.

1. In the window from which you want to export data, click the **Save to file** icon at the top right.



A report containing the visible data opens in a new window, as shown in the following example.



2. To save the report to a file:
  - a. Click the save icon at the top-left of the report viewer.
  - b. In the **Save** window, navigate to the location where the file is to be stored.
  - c. In the **File Name** field, type a name for the report.
  - d. From the **Files of Type** list, select the format for the report.
  - e. Click **Save**.
3. To email the file to one or more recipients, click **Send as Email Attachment**, provide the address of each recipient, then click **OK**.
4. You can use the paging controls to move through a multi-page document.
5. You can use the viewing controls to increase or decrease the size of the displayed data.
6. To close the report viewer, click the close button (X) at the top right of the window.

## 2.5 Set preferences

Use this procedure to set the following NOC preferences:

- **General** — Sets the general preferences for ToolTips and time formats, as described in the table “[General NOC preferences](#)” on page 26.
- **Email SMTP Settings** — Defines the email encryption and authentication protocol to be used for the client SMTP mail server that will be used to email exported reports, as described in the table “[Email SMTP Settings](#)” on page 28.
- **Navigation** — Sets preferences for how the network element data is loaded and displayed in the NOC navigation panel. See the table “[Navigation preferences](#)” on page 28 for a description of the options.
- **Topology** — Sets the default topology layer that is displayed when you log in to the NOC and determines whether off-page connectors are displayed.
- **Network Element View** — Determines whether slots are shown in the Resource Tree in the Network Element View window.

NOC preferences are stored on a per-system basis. Any preferences that you define using this procedure will apply to any NOC user who logs on to this computer.



Note: There is also a tab for SONET Domain Manager preferences. This only applies if you have installed NI-Director SONET Domain Controller (SDC). See the SDC documentation for more information.

**Table 2–4: General NOC preferences**

Preference	Description
Tooltip Initial Delay	Controls the time (in milliseconds) that the cursor must hover over a UI object before the associated tooltip will be displayed. The changes for tooltip take effect immediately. Default: 250 milliseconds
Tooltip Dismiss Delay	Specifies the amount of time (in milliseconds) that the tooltip will be displayed for before it is removed. The changes for tooltip take effect immediately. Default: 30000 milliseconds
Time Zone	Specifies the time zone that the NOC should convert all dates and times to before displaying them. All geographic time zones are listed. The changes take effect immediately.

Preference	Description
Date and Time Format	<p>Defines the format for displaying the date and a time in the NOC user interface, as follows:</p> <p><b>yyyy/MM/dd hh:mm:ss</b>  <b>yyyy/MM/dd HH:mm:ss z</b>  <b>yyyy/MM/dd HH:mm:ss.SSS</b>  <b>yyyy/MM/dd HH:mm:ss.SSS z</b>  <b>yyyy/MM/dd hh:mm:ss a</b>  <b>yyyy/MM/dd hh:mm:ss a z</b>  <b>yyyy/MM/dd hh:mm:ss.SSS a</b>  <b>yyyy/MM/dd hh:mm:ss.SSS a z</b>  <b>MM/dd/yyyy HH:mm:ss</b>  <b>MM/dd/yyyy HH:mm:ss z</b></p> <p>where:</p> <p><b>yyyy</b>=year, such as 2007  <b>MM</b>=month, such as 12  <b>dd</b>=day, such as 07  <b>HH</b>=24-hour format (00-24), such as 13  <b>hh</b>=12-hour format (00-12), such as 01  <b>mm</b>=minutes, such as 53  <b>ss</b>= seconds, such as 09  <b>SSS</b>=milliseconds, such as 123  <b>z</b>=time zone, such as GMT</p> <p>The changes take effect immediately.</p>
Clock Format	<p>Defines the format for the clock display, as follows:</p> <p><b>HH:mm</b>  <b>HH:mm:ss</b>  <b>HH:mm:ss z</b>  <b>HH:mm z</b>  <b>hh:mm a</b>  <b>hh:mm:ss a</b>  <b>hh:mm a z</b>  <b>hh:mm:ss a z</b></p> <p>where:</p> <p><b>a</b>=displays AM or PM for the 12-hour clock</p> <p>for explanations of the other formats, see “Date and Time Format”</p> <p>The changes take effect immediately.</p>

**Table 2–5: Email SMTP Settings**

<b>Preference</b>	<b>Description</b>
Server Hostname	The hostname of the client mail server that will be used for mailing reports
Server Port	The port on the mail server
Authentication	Defines the email encryption and authentication protocol to be used: Not_Applicable, Basic, TLS, or SSL. If you select Basic, TLS or SSL, you must specify the User ID and User Password in the corresponding fields.

**Table 2–6: Navigation preferences**

<b>Preference</b>	<b>Description</b>
a - Load All Network Elements at Login	If this option is selected, all the NEs in the network will be loaded into memory at log in time. If this option is not selected, then the NEs are loaded into memory the first time you click on an NE group in the navigation panel. <b>Caution:</b> Select this option with caution. If there are a large number of NEs in the network, it will take longer to log in to the NOC because of the large amount of data to be loaded. If you want to reduce the time it takes to log in to the NOC, leave this option deselected.
b - Show Network Elements in Contained NE groups	If this option is selected, when you click on a container group in the navigation tree that contains other NE groups, all NEs contained in the NE groups are loaded into memory and displayed in the Network Elements table. If this option is not selected, the NEs are loaded into memory, but NEs are only displayed in the Network Elements table when you click on a static or dynamic NE group within the container.
c - Show Network Elements in Network group	If this option is selected, clicking on the top level Network group in the navigation panel will display all the NEs in the network in the Network Elements table. If this option is not selected, clicking on the top level Network group in the navigation panel will not display any NEs in the Network Elements table.
When deciding on which Navigation preferences to set, consider the following: Selecting both b and c is functionally equivalent to selecting only a. The difference is the point at which the data is loaded into memory. If both b and c are selected, the data is loaded into memory only when you click on an NE group in the navigation panel. If a is selected, the data is loaded into memory at log in time.	

1. On the **File** menu, select **Preferences**.

The Preferences window opens.

### General tab: Set tooltip and time preferences

2. Click the **General** tab and set the preferences as described in the table “[General NOC preferences](#)” on page 26.
3. Select another tab, or click **OK** to save the changes, or click **Cancel** to exit without saving the changes.

### Email SMTP Settings tab: Configure email

4. Click the **Email SMTP Settings** tab and set the preferences as described in the table “[Email SMTP Settings](#)” on page 28.
5. Select another tab, or click **OK** to save the changes, or click **Cancel** to exit without saving the changes.

### Navigation tab: Configure how NE data is loaded

6. Click on the **Navigation** tab and define the preferences as described in the table “[Navigation preferences](#)” on page 28.
7. Select another tab, or click **OK** to save the changes, or click **Cancel** to exit without saving the changes.

### Topology tab: Choose the default topology layer and set the off-page connector view

8. Click on the **Topology** tab.
9. From the **Default Layer** list, choose one of the following layers to display by default when you log in to the NOC:
  - All Layers
  - NE to NE

For more information about the topology layers that are available, see “[About network topology layers](#)” on page 35. Your choice will be displayed the next time you log in to the NOC. It will also be displayed if another user logs in to the NOC using the same computer.

If you do not choose a default topology layer, All Layers is used.

If you select another layer while viewing a group, that layer will be saved for the group. This is only saved on a per-user basis, not for the system. Other users logging in to the NOC on this system will not see the same layer selection.

10. If you want to display off-page connectors, select the **Show Off-Page Connectors** check box.

If you enable this check box, off-page connectors will be shown when an NE is connected to an NE in a group not currently shown in the Topology view. See “[Topology view](#)” on page 34 for an example.

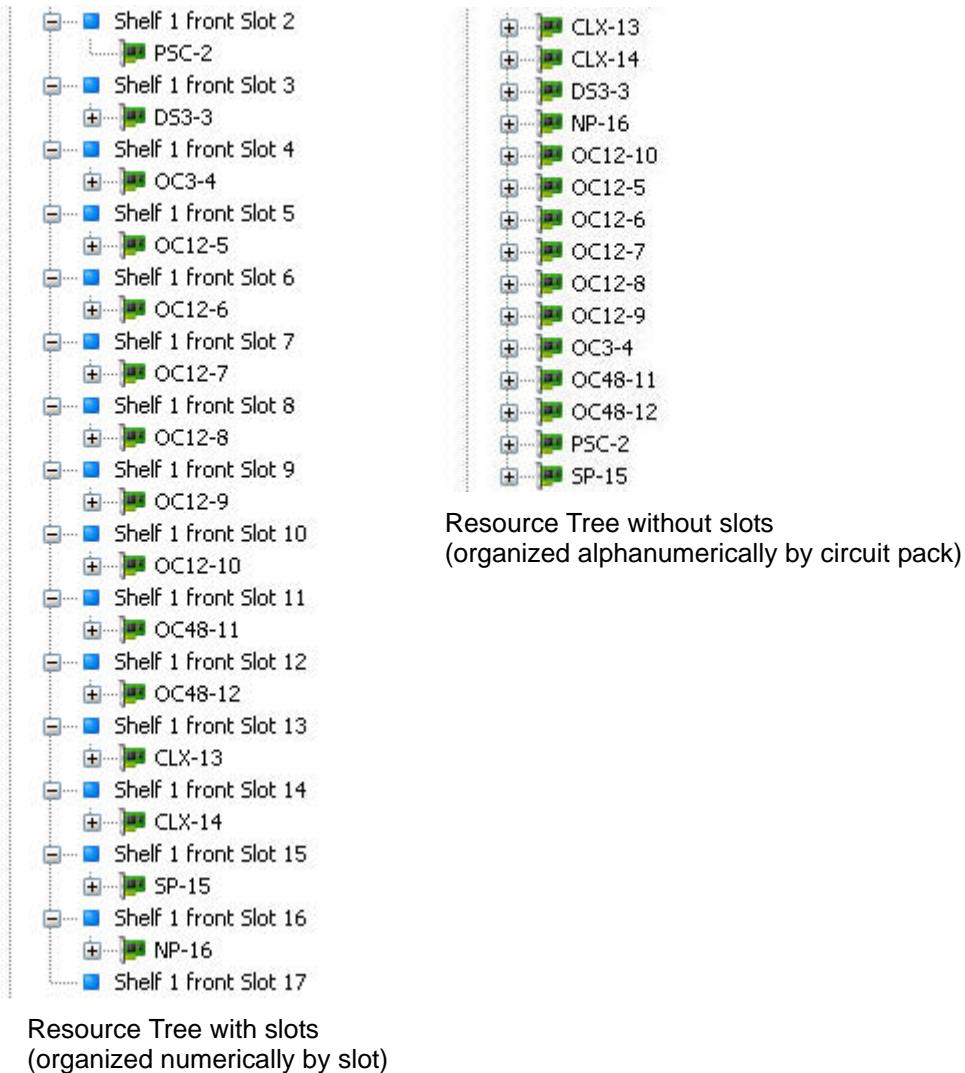
### Network Element View tab: Choose whether to display slots

11. Click on the **Network Element View** tab.
12. If you do not want to display slots in the Network Element View window, clear the **Show Slots in Tree** check box.

By default, it is enabled. If you have a Network Element View window open and you change this setting, you can click the Refresh button in the Network Element View window to update the Resource Tree with the new view (see “[Update inventory in the Network Element View window](#)” on page 52).

The following image shows the same shelf with slots displayed and not displayed.

Note: If Show Slots in Tree is enabled, then empty slots are shown in the tree. Otherwise, they are not.



13. Select another tab, or click **OK** to save the changes, or click **Cancel** to exit without saving the changes.
14. To see the changes take effect, exit from the NOC, then re-launch the NOC.

## 2.6 View plugin details

Use the following procedure to see information about the plugins that are installed with the NOC.

1. On the **Help** menu, click **System and Application Properties**.

The System and Application Properties window opens.

2. Click the **Plugins** tab.

Details about plugin are listed.

3. Click the Close (X) button to close the window.

## 2.7 Launch Network Integrity framework applications

You can launch Network Integrity framework applications from a number of locations in the NOC. For example, as described in “[Actions available in the groups navigation tree](#)” on page 15, choosing Edit Group opens the NE Group Manager for the group that you chose. You are automatically logged in to the Network Integrity with your current NOC credentials.

Other access points are described throughout this guide, where applicable.

For detailed information about how to use the Network Integrity Framework, launch the online help. From the **Help** menu, select **Contents**.



**Note:** Nakina Systems supports the use of Internet Explorer version 8 or 9 with the Google Chrome Frame plugin or Mozilla Firefox 8 or higher as the web browsers for using the Network Integrity framework applications.

## 2.8 Log out

Use the following procedure to exit and log out of the NOC.

1. On the **File** menu, click **Exit**.

All the windows in the NOC close and your user session is terminated.

## 2.9 Change your password

Use this procedure to change the password for your Network Integrity account. The ability for you to change your own password is configurable by your network administrator through the “User Administration Role” with the permission set to "Allows user to modify their own password".



**Note:** You can log into the NI-Director Operations Console, NI-Guardian and Network Integrity applications with the same Network Integrity account. Speak to your network administrator for more information.

1. On the **File** menu, select **Change Password**.

The Change password window opens.

2. Enter values in the **Old Password**, **New Password**, and **Confirm New Password** fields.

3. Click **OK**.

Your Network Integrity password has been changed.

## 3 Viewing network topology

Network topology is a graphical representation of network connectivity in an NE group.

This section describes the Topology view ([“About the Topology view” on page 33](#)) and provides the following procedures for working with topology:

- “View topology for an NE group” on page 37
- “View topology for a specific layer” on page 37
- “Refresh the Topology view” on page 38
- “View topology for an NE” on page 38
- “Add a background image to the Topology view” on page 38
- “Reposition NEs in the Topology view” on page 39
- “View NE equipment details” on page 40
- “View group details” on page 41

You can also monitor alarms using the Topology view. For alarm monitoring procedures, see [“Monitoring the network for alarms” on page 58](#).



**Note:** If while using the NOC you do not see menu items, tabs or buttons that are described in this documentation, it is because the Network Integrity administrator has not assigned the permission to your user account, or the feature has not been installed.

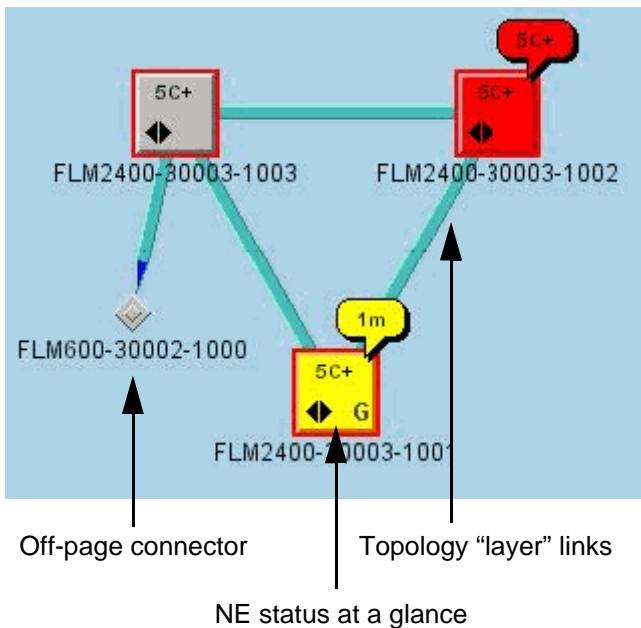
### 3.1 About the Topology view

When you select a container group in the groups navigation tree, the Topology view shows the groups within the container group. When you select a static or dynamic group, the Topology view shows:

- a graphical representation of the NEs in the group
- NE connectivity

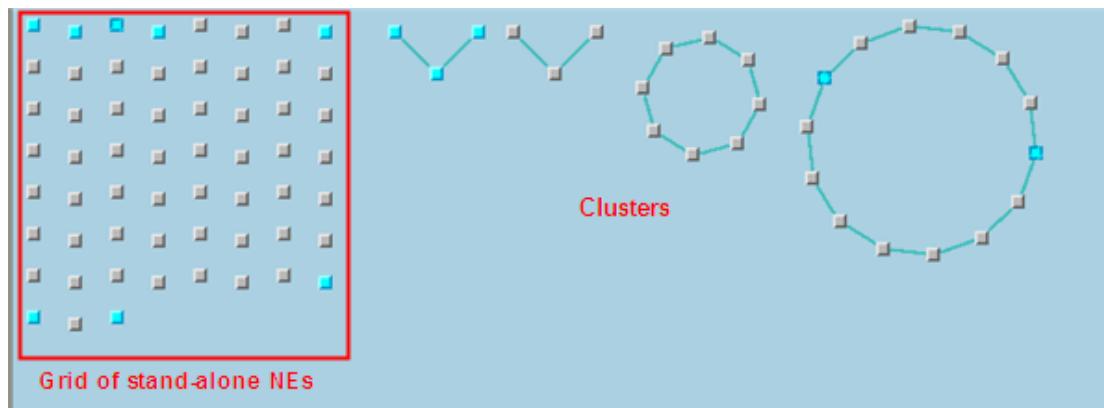
[“Topology view” on page 34](#) explains the components of a typical Topology view.

If an NE is connected to an NE in a group not currently shown in the Topology view, and you have chosen to display off-page connectors (described in [“Topology tab: Choose the default topology layer and set the off-page connector view” on page 29](#)) an off-page connector icon is displayed. To display the NE group associated with the off-page connector, right click the off-page connector and select Topology > Open Topology > In Main Window (or In New Window) and then select the name of the NE Group that contains the NE.

**Figure 3–1: Topology view**

By default, the NOC positions the network elements in the Topology view as follows:

- The stand-alone NEs are positioned first. They are placed alphabetically starting from top left to right, and then from top to bottom. Gateway NEs (indicated by the letter “G”) are shown first.
- Clusters of NEs are displayed to the right of any stand-alone NEs. For linear clusters, the GNE appears to the left of the chain of NEs.

**Figure 3–2: Default layout**

When new NEs are added to the system, they are positioned according to the defaults. You can permanently change the default layout by moving the NEs to the desired positions, then saving the layout. See “[Reposition NEs in the Topology view](#)” on page 39.

You can temporarily reposition the NEs without saving. In this case, when you deselect the group (by ctrl-clicking on it or by selecting a new group) or refresh the graphic, the

positions are saved locally. When the group is selected again, the local positions will then be used. These positions will be used until the NOC is closed.

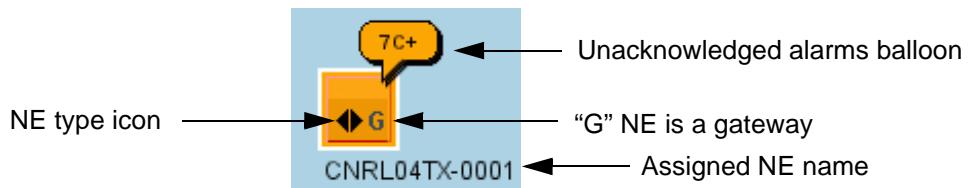
### 3.1.1 About NE status at a glance

The NOC uses colored icons and text to represent the status and type of NEs in the network:

- Each NE is identified in the Topology view by the assigned NE name
- The letter “G” indicates a gateway NE.
- The NE type icon is an industry standard icon. For more information on what the icons represent, see [“NE icons in the Topology view” on page 224](#).

You can move your mouse over the NE type icon to see a text description of the NE type.

For an explanation of the alarm color coding and the alarm balloon, see [“Understanding alarm colors and values” on page 59](#).



### NE states

NE states are represented in the Topology view as follows:

- NR — indicates that the NE is not reporting faults
- ? — indicates that the NE is unmanaged
- light blue — indicates that the NE is out of contact
- small clipboard icon — indicates that the NE is under test

### 3.1.2 About network topology layers

The NOC shows network topology at different layers based on the data that is available from the NE or the network configuration. The topology data is retrieved and calculated when data mining is performed with the Network Integrity Framework. In order to retrieve the required data for the Topology view, the “Retrieve Logical Resources” option must be selected when data mining is performed. See the Network Integrity Framework Configuration Guide for more information.

Interfaces are modeled in Network Integrity as trail termination points (TTPs), which are the terminations of transmission paths at specific network layers. The Topology view in the NI-Director Operations Console is built by linking TTPs together. When Network Integrity determines that a TTP on one NE is the far-end of a TTP on another NE, a topology link is created. The links can be viewed by selecting the appropriate layer.

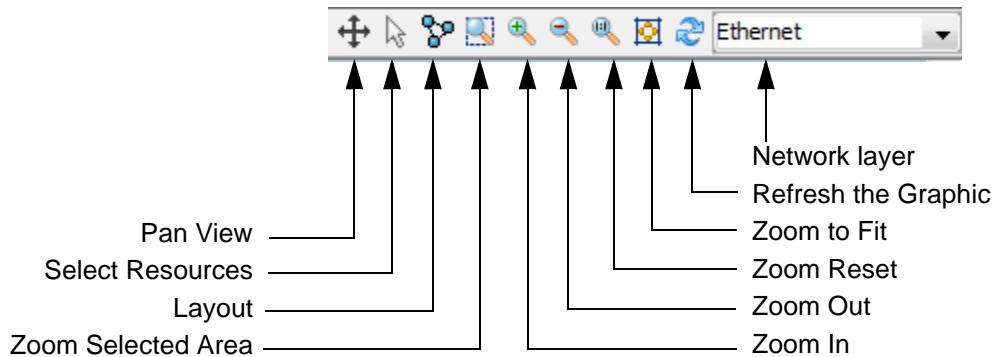
The list of topology layers that is shown in the Topology window contains only the layers that are supported in the selected group. For example, if the group supports Ethernet, then Ethernet is displayed in the layers list. The layer list always contains:

- All Layers — displays all connections between NEs regardless of the network layer in which they occur
- NE to NE — displays manual topology links created using the Link Manager. These links are not created by Network Integrity. For more information about manual topology links, see “[Managing links](#)” on page 165.

### 3.1.3 Topology view controls

The Topology view can be controlled using the toolbar buttons.

**Figure 3–3: Topology view toolbar buttons**



The toolbar buttons (from left to right in the figure) are described in “[Toolbar button descriptions](#)” on page 36.

**Table 3–1: Toolbar button descriptions**

Button	Description
Pan View	When you click this button, the cursor changes to a hand and enables you to move the entire image around in the Topology window.
Select Resources	When you click this button, the cursor changes back to an arrow to allow you to select items.
Layout	When you click this button, the system arranges the NEs on the screen according to the default layout rules (shown in “ <a href="#">Default layout</a> ” on page 34). This can be useful if you have rearranged a number of NEs, but want to return to a default layout. (The layout button will not permanently alter the layout of saved node positions. As soon as a refresh is performed, the NEs will return to their saved positions.)
Zoom Selected Area	The cursor changes to a magnifying glass and can be used to drag-select an area of the Topology view to increase its size.
Zoom In	Magnifies the current Topology view including any background image. (When you zoom in, the NE icons don't increase in size, but the links between the NEs increase.)

Button	Description
Zoom Out	Decreases the current Topology view including any background image. (When you zoom out, both the NE icons and the links decrease in size.)
Zoom to Fit	Scales the current Topology view to fit the available screen size.
Zoom Reset	Returns a zoomed image to its original size.
Refresh the Graphic	Update the Topology view with the latest information in the Network Integrity database.
Network layer	Displays the connections between NEs in the selected layer type (see <a href="#">"About network topology layers" on page 35</a> for more information about network layers). The Network Layer selection persists for each NOC session.

## 3.2 View topology for an NE group

Use this procedure to display a graphical view of the topology for an NE group.

When the NOC is first launched, the NE groups to which you have access appear in the groups navigation tree.

The topology layer that is displayed for the group is the default that you chose in ["Topology tab: Choose the default topology layer and set the off-page connector view" on page 29](#). If you did not choose a default layer, "All Layers" is displayed.

1. To display the topology for an NE group in the main window, select the group in the groups navigation tree.  
After a brief retrieval period, the topology for the selected group is displayed in the Topology view, as shown ["Topology view" on page 34](#).  
For an explanation of the different icons, see ["About NE status at a glance" on page 35](#).
2. To display topology for an NE group in a new window, right-click the group in the Topology view or in the groups navigation tree and choose **Topology > In New Window**.

## 3.3 View topology for a specific layer

Use this procedure to display the connections between NEs at a specific layer. For a description of how topology is modeled, see ["About network topology layers" on page 35](#).

When you select a layer for a group, that layer is saved and is displayed each time you select the group. If you change the layer, the new selection is saved. This is only saved on a per-user basis, not for the system. Other users logging in to the NOC on this system will not see the same layer selection.

1. ["View topology for an NE group" on page 37](#).
2. Select a layer that you want to view from the layer menu.

The NOC displays the Topology view for the selected layer. If there are no connections at the selected layer, there will be no connection lines drawn between the NEs.

## 3.4 Refresh the Topology view

Use this procedure to refresh the Topology view with the latest NE attributes and neighbor attributes collected from the Network Integrity database.

1. [“View topology for an NE group” on page 37.](#)
2. Click the **Refresh the Graphic** icon at the top right of the Topology view.



Refresh the Graphic

The Topology view is updated with the latest information from the Network Integrity database.

## 3.5 View topology for an NE

If an NE is a member of more than one group, you can use this procedure to display the topology for any of the other groups.

1. In the Network Elements table or the Topology view, right-click on the network element and select either of the following options:
  - **Topology > Open Topology > In Main Window**, followed by the group name
  - **Topology > Open Topology > In New Window**, followed by the group nameThe first option opens the group topology in the main Topology window.  
The second option opens the group topology in a new standalone Topology window. This can be useful for comparing Topology views.

## 3.6 Add a background image to the Topology view

Use this procedure to add a graphic image, such as a map, to the topology background to provide context for the location of network elements. When the background image is set for an NE group, any NOC user who logs into Network Integrity and is authorized to select the group will see the image until the image is cleared.



Note: Background image files should be no larger than 2 MB. Files larger than this can cause performance issues and timeouts while being loaded.

1. [“View topology for an NE group” on page 37.](#)
2. Reset the zoom by clicking the **Zoom Reset** icon in the Topology toolbar.  
This will allow the image to be imported at its regular size. If the current Topology view is zoomed in or out, the image will be imported and zoomed accordingly.
3. Right-click the topology background and select **Set Background Image**.

4. Navigate to the folder where the desired image (GIF JPG, or PNG) is stored, select it, and then click **Open**.

The NOC displays the selected image as the background of the Topology view.

To position nodes over the image, see “[Reposition NEs in the Topology view](#)” on page 39.

#### To remove the background image

5. Right-click the topology background and select **Clear Background Image**.

## 3.7 Reposition NEs in the Topology view

Use this procedure to place network elements in specific positions in the Topology view and then save the layout. This is useful to keep network elements properly positioned over a map or similar background image.



**Note:** You can temporarily reposition the NEs without saving. In this case, when you deselect the group (by ctrl-clicking on it or by selecting a new group) or refresh the graphic, the positions are saved locally. When the group is selected again, the local positions will then be used. These positions will be used until the NOC is closed.

When the node positions are saved for an NE group, any NOC user who logs into Network Integrity and is authorized to select the group will see the nodes in the set position.

1. “[View topology for an NE group](#)” on page 37.

#### To reposition NEs in the Topology view

2. Click and drag each network element to the desired position.

To select multiple NEs, hold down the Shift key while clicking.

#### To Lock the NE position over the image

3. When the NEs are in position, right-click the topology background and select **Save Node Positions**. If you don't save, the NEs to their default positions if the NOC is closed and reopened.



**Note:** Once saved, all NOC users who have access to the selected NE group will see the node positions change in their NOC Topology view.

#### To clear the position of the nodes

4. Right-click the topology background and select **Clear Node Positions**.

## 3.8 View NE equipment details

Use this procedure to view details about a network element by selecting it in the Network Elements table or the Topology view. The information contained in the Details window includes:

Name	Provides the name of the network element.
Vendor	Identifies the vendor of the network element.
Model	Identifies the model of the network element.
Software Version	Identifies the software version on the network element.
Type	Identifies the type of network element.
Management Addresses	If applicable, shows the IP or OSI address of the network element.
CLLI	If applicable, identifies the alphanumeric common language location identifier (CLLI) of the network element.
Administrative State	If applicable, identifies the administrative state of the network element, which is typically a state set by a user, such as: Locked, Unlocked or Shutting Down. If the state is not known, the system reports the state as Unknown.
Management State	Identifies the current management state of the network element, for example, Managed, Unmanaged or Under Test.
X Coordinate	One of two physical coordinates to identify the location of the NE. The coordinate is optional and was assigned to the NE when it was brought under management by Network Integrity.
Y Coordinate	One of two physical coordinates to identify the location of the NE. The coordinate is optional and was assigned to the NE when it was brought under management by Network Integrity.
Last Updated (Physical)	Shows the date and time when the physical inventory was last updated.
Last Updated (Logical)	Shows the date and time when the logical inventory was last updated.
Last Updated (Service)	Shows the date and time when the service inventory was last updated.
Location	Describes the physical location of the NE.
Manufacture Date	Shows the date that the NE was manufactured.
Communication State	Identifies the current state of communication with the NE, for example, In Contact or Out of Contact.
Adapter	Identifies the adapter that has been assigned to the NE.

If any of this information is not provided by the NE, the fields are either blank or show "Not Reported".

1. In the Network Elements table or the Topology view, click the network element for which you want to see details.
2. Do one of the following:
  - a. Click the **Details** tab at the bottom of the window.

- The NE details are displayed.
- Right-click on the NE and select **Inventory > Details**.

The Network Element Details window opens.

By clicking the menu arrow, you can perform a number the same tasks as you can from the Network Elements table. See “[Actions available in the Network Elements table](#)” on [page 18](#) for more information.



**Note:** You can obtain NE attributes directly from the NE instead of from the Nakina database and display them in a separate window. To do so, right-click the NE in the Network Elements table or Topology view and choose **Inventory > View Attributes From Network**.

## 3.9 View group details

Use this procedure to view details about a group by selecting it in the groups navigation tree or the Topology view. The information contained in the Details window includes:

Name	Provides the name of the group.
Type	Indicates the type of group (static, dynamic, or container). For details about group types, see the Network Integrity Framework Configuration Guide.
Parents	Identifies the parent groups of the selected group.
Number of Parent Groups	Indicates the number of groups that contain the selected group.
Number of Children Groups	Indicates the number of groups within the selected group.
Number of Network Elements	Indicates the number of network elements within the selected group.

- Do one of the following:
    - In the Topology view, click the group for which you want to see details, then click the **Details** tab at the bottom of the NOC window.
- The group details are displayed.
- In the groups navigation tree or in the Topology view, right-click on the group or which you want to see details and select **Inventory > Details**.
- The Group details window opens.



By clicking the menu arrow, you can perform a number the same tasks as you can from the Groups navigation tree. See “[Actions available in the groups navigation tree](#)” on [page 15](#) for more information.

## 4 Viewing shelf level graphics

---

This section contains procedures for troubleshooting NEs at the shelf level and below. You can start with an overall network topology view that shows network connectivity and alarms at a glance, and then drill down to view shelves, circuit packs, ports, and interfaces. (See “[Viewing network topology](#)” on page 33 for details about the Topology view.)

Shelf level graphics (SLG) are displayed in the Network Element View window. This section provides an overview of the Network Element View window (“[About the Network Element View window](#)” on page 42) and the following procedures:

- “[View shelf, circuit pack, port, and interface details](#)” on page 48
- “[Update inventory in the Network Element View window](#)” on page 52

For alarm monitoring procedures, see “[Monitoring the network for alarms](#)” on page 58.



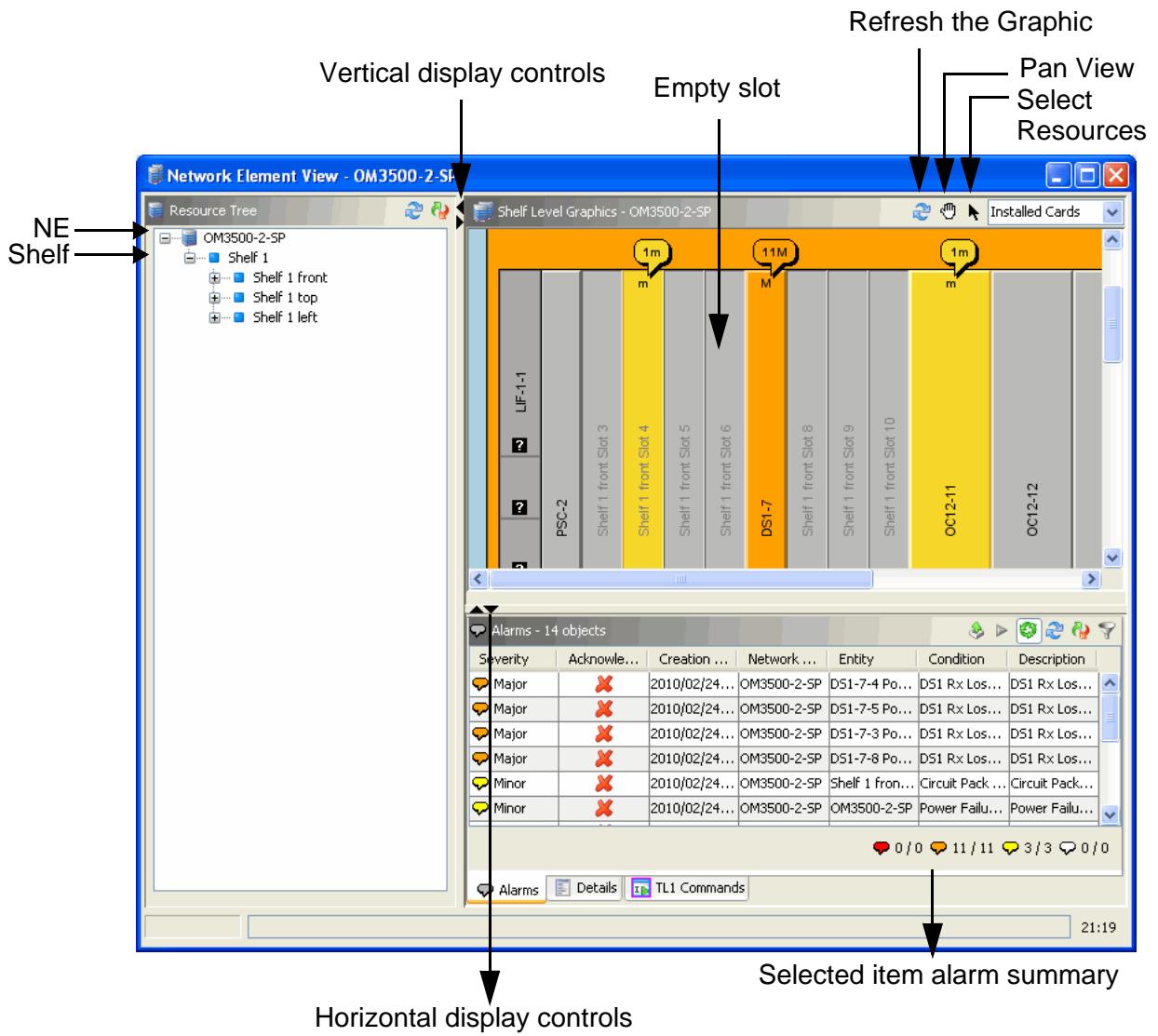
**Note:** If while using the NOC you do not see or cannot access menu items, tabs or buttons that are described in this documentation, it is because the Network Integrity administrator has not assigned the permission to your user account, or the feature has not been installed.

### 4.1 About the Network Element View window

The Network Element View window shows the shelves, slots, circuit packs, ports, and interfaces that are housed in the NE. The view shows gray boxes or can be a more realistic representation of the shelf, depending on how the adapter was created.

Navigation within the Network Element View window is similar to the main NOC window in that items are selected in the Resource Tree or in the Shelf Level Graphics view. Operators can immediately see alarmed circuit packs in the shelf, select the circuit pack and see the alarm details.

Figure 4–1: Network Element View window features



For examples of how to interpret circuit pack icons, see “[Sample NE and circuit pack alarm conditions](#)” on page 60.

The time shown is the time from the PC where the NOC is currently running.

The following image controls are available in the Shelf Level Graphics view.

Pan View	When you click this button, the cursor changes to a hand and enables you to move the entire image around in the Shelf Level Graphics view.
Select Resources	When you click this button, the cursor changes back to an arrow to allow you to select items.

### 4.1.1 About slot states

Circuit packs are identified as expected and/or installed. If a circuit pack is provisioned, it is expected. If it is actually present in the system, it is installed.

If a slot does not contain a circuit pack, it is shown as empty. Depending on the expected and installed state of the slot, it may also appear with a question mark or an X.

The following table shows a cross-reference of how a slot is represented according to expected and installed state. For example, if a slot is empty and the system expected it to be empty, then just the slot is displayed. If the slot is empty and the system expected a circuit pack, then the circuit pack and the  symbol are displayed.

**Table 4–1: Slot states**

Slot holder state	Expected No Circuit Pack	Expected Circuit Pack	Installed No Circuit Pack	Installed Circuit Pack
Not Applicable	slot	circuit pack 	slot	circuit pack 
Empty (Not Installed and Not Expected)	slot	circuit pack 	slot	circuit pack 
Expected and Not Installed	slot	slot	slot 	circuit pack
Installed and Not Expected	slot 	circuit pack	slot	slot
Installed and Expected	slot 	circuit pack	slot 	circuit pack
Mismatch Installed-Expected	slot 	circuit pack 	slot 	circuit pack 
Unavailable	?	?	?	?
Unknown	slot	circuit pack 	slot	circuit pack 

You can “[View shelf, circuit pack, port, and interface details](#)” on page 48 to confirm the administrative and operational state of the circuit pack.

### 4.1.2 About circuit pack states

Depending on the administrative and operational state of the circuit pack, it may be grayed out, have a dashed outline, or appear with a lock icon or a question mark. The following table shows a cross-reference of how a circuit pack is represented according to administrative or operational state.

**Table 4–2: Circuit pack states**

<b>Administrative state</b>	<b>Operational state</b>	<b>Graphical indication</b>
Locked	Enabled	Grayed out █
Unlocked	Enabled	None
Shutting Down	Enabled	█
Unknown	Enabled	Grayed out ?
Locked	Disabled	Grayed out, with dashed outline █
Unlocked	Disabled	Grayed out, with dashed outline
Shutting Down	Disabled	Grayed out ?
Unknown	Disabled	Grayed out ?
Locked	Unknown	Grayed out ?
Unlocked	Unknown	Grayed out ?
Shutting Down	Unknown	Grayed out ?
Unknown	Unknown	Grayed out ?

### 4.1.3 Circuit pack and slot state examples

This example shows how circuit packs are represented in the Expected and Installed views. In the following example:

- slots 1-6, 8-12, and 16 are Expected and Not Installed
- slot 7 is Installed and Expected
- slots 13-17 and slot 17 are empty

### Installed view

In this view:

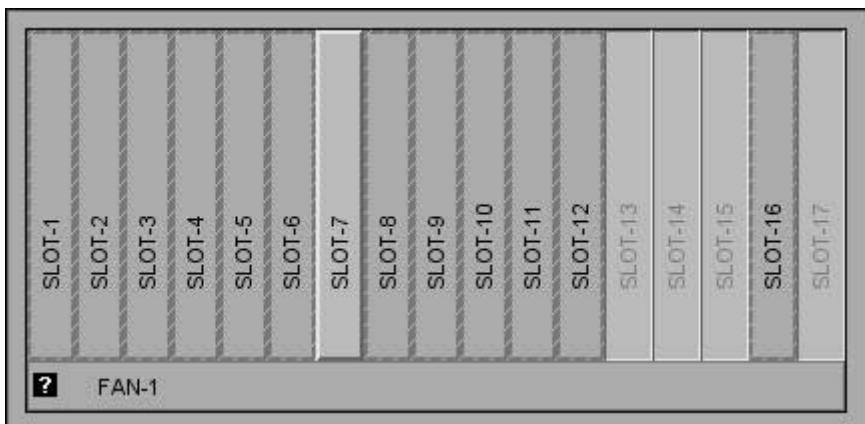
- slots 1-6 and 8-17 are shown as empty slots (they appear as 2-dimensional and the text label is gray)
- slot 7 contains a circuit pack with an administrative state of Unlocked and an operational state of Enabled (it appears as 3-dimensional and the text label is black)



### Expected view

In this view:

- slots 1-6, 8-12, and 16 contain circuit packs (the text label is black)  
These circuit packs have an operational state of Disabled (they appear as 2-dimensional, with dashed outlines)
- slot 7 contains a circuit pack (the same as the Installed view) with an operational state of Enabled
- slots 13-15 and slot 17 are empty



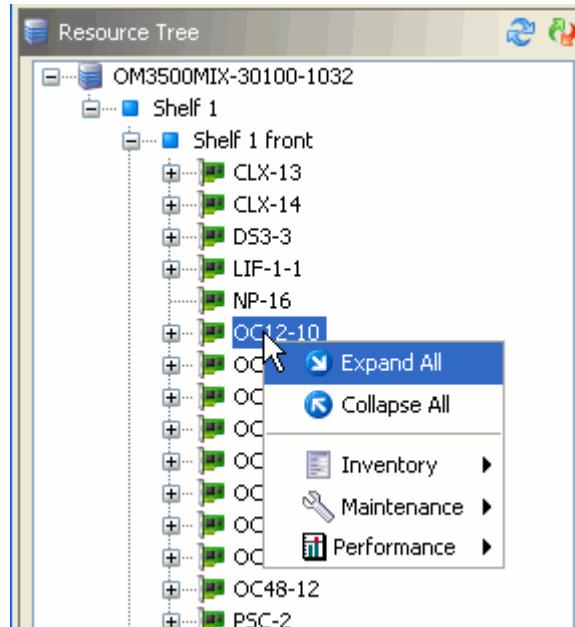
## 4.1.4 About the Resource Tree

As shown in “[In-context menu selections](#)” on page 47, menu selections are available in context with the item currently selected in the Resource Tree.



Note: The view in the Resource Tree will be different depending on whether you have chosen to display slots. See “[Set preferences](#)” on page 25 for more information.

**Figure 4–2: In-context menu selections**



You can choose the Expand All option at any level in the Resource Tree to expand all items within the selected item.

The following icons are shown in the Resource Tree:

	Shelf and slot icon — Expand slots to view circuit packs.
	Circuit pack icon — Expand to view contained ports and interfaces.
	Port icon — Expand ports to view interfaces.
	Interface icon — Expand interfaces to view interfaces below the current interface.

#### 4.1.5 About the display controls

You can control which sections of the Network Element View to hide or display using the display controls provided. The display controls are arrows located between the sections of the Network Element View window. See “[Network Element View window features](#)” on

[page 43](#) for details on the location of the display controls. The following table explains the function of the controls.

Icon	Use
	Vertical Display Controls — When all frames are displayed, click the left arrow (the top arrow) to hide the Resource Tree. To display it again, click the right arrow (the bottom arrow). When all frames are displayed, click the right arrow to hide the Shelf Level Graphics frame and the Alarms frame. Click the left arrow to display them again.
	Horizontal Display Controls — When all frames are displayed, click the up arrow to hide the Shelf Level Graphics Frame. To display it again, click the down arrow. When all frames are displayed, click the down arrow to hide the Alarms frame. Click the up arrow to display it again.

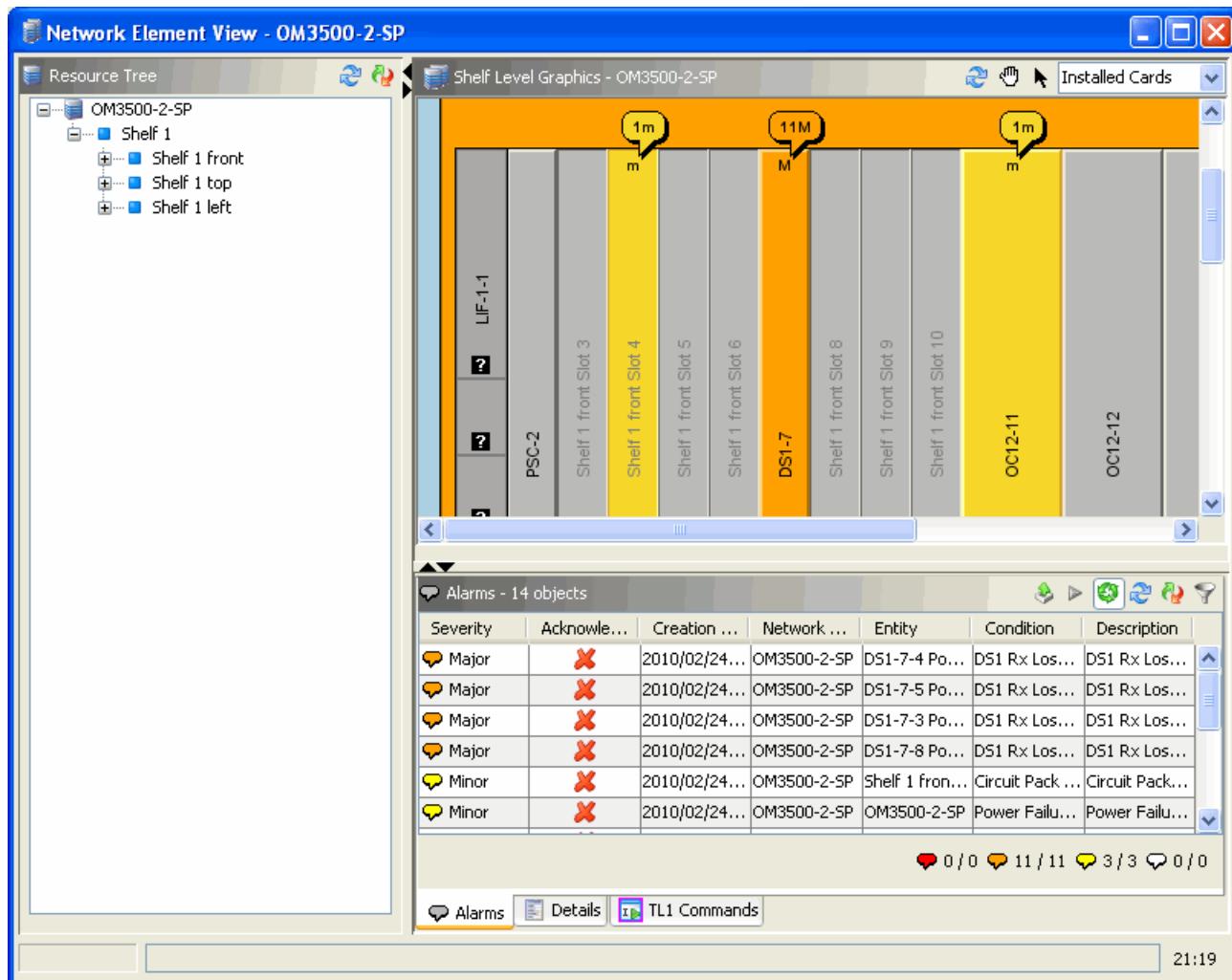
If you change the display or resize the sections of the window, the changes are saved and the window is displayed the same way the next time you log in to the NOC. Other users of the NOC, whether on the same machine or not, will not see your changes.

## 4.2 View shelf, circuit pack, port, and interface details

Use this procedure to drill down into an NE and display a graphical view of the shelves on the NE. If any circuit packs in a shelf have alarms, the circuit pack is color-coded to indicate the alarm severity.

1. In the Network Elements table or in the Topology view, right-click an NE and select **Shelf Level Graphics** from the menu.  
Alternatively, you can double-click an NE to open the shelf level graphics view.

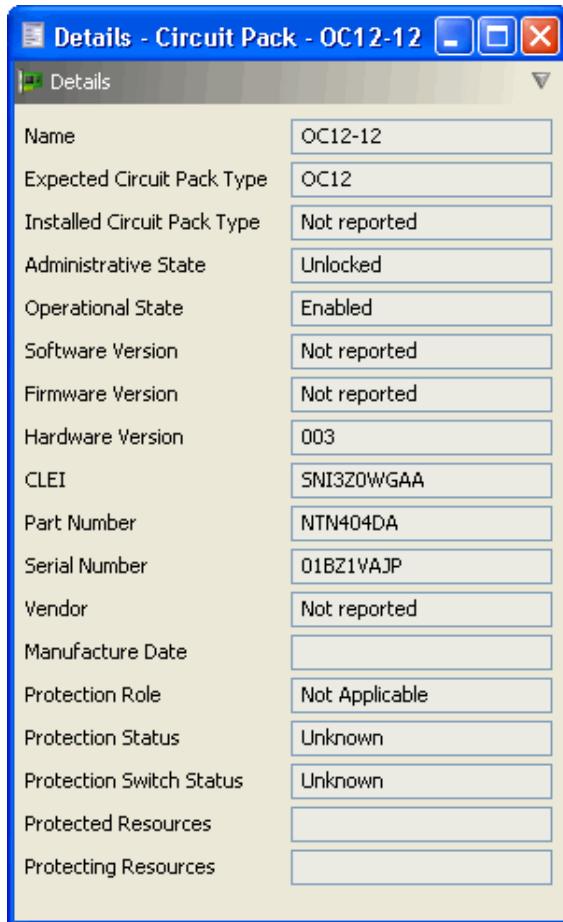
The system displays the Network Element View for the selected NE. The Shelf Level Graphic for the selected shelf is displayed on the right side of the window.



By default, installed circuit packs are shown. If you want to view expected circuit packs, choose Expected Cards from the top right menu.

2. To view alarms for the shelf or one of its components, select the desired item in the Resource Tree and then click the **Alarms** tab.
  3. To view details for the shelf or one of its components, select the desired item in the Resource Tree and then click the **Details** tab.
- You can expand the Resource Tree and select down to the interface level.
4. To view details for a circuit pack, do one of the following:
    - Click the circuit pack in the Resource Tree or shelf level graphics view and then click the **Details** tab.

- To view details in a new window, right-click on a circuit pack in the Resource Tree or shelf level graphics view and select **Inventory -> Details**. The system displays the details in a new window.



You can obtain circuit pack attributes directly from the network instead of from the Nakina database and display them in a separate window. To do so, click the menu arrow in the Details window and choose **View Attributes From Network** or right-click on a circuit pack in the Resource Tree or shelf level graphics view and select **Inventory -> View Attributes From Network**.

If the NE is out of contact, this option is not available.

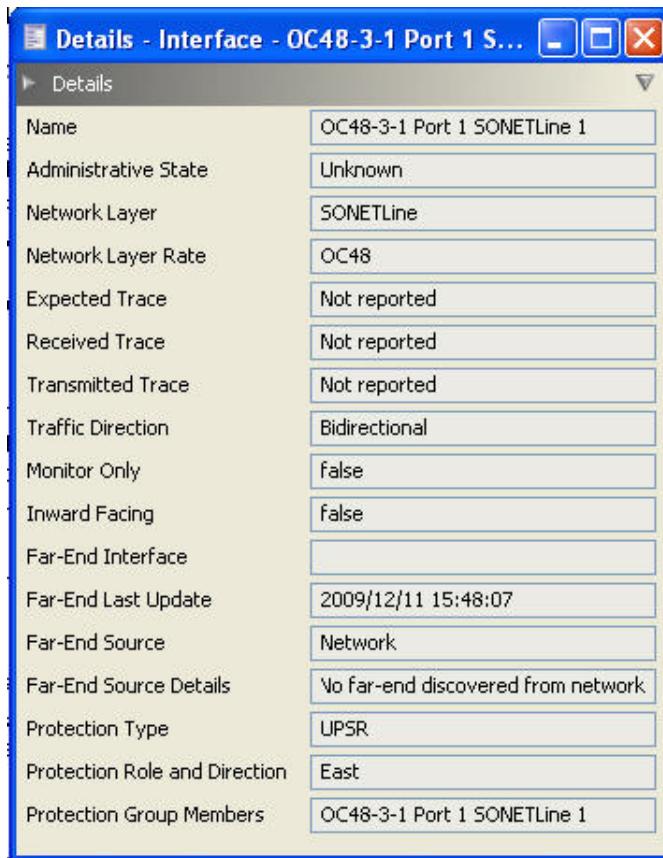
5. To view details for a port, expand the circuit pack on which the port resides in the Resource Tree and do one of the following:
  - Click the port in the Resource Tree then click the **Details** tab.
  - To view details in a new window, right-click the port in the Resource Tree and select **Inventory -> Details**. The system displays the details in a new window.

Details for a port include the name, administrative and operational states, and protection information.

You can obtain port attributes directly from the network instead of from the Nakina database and display them in a separate window. To do so, click the menu arrow in the Details window and choose **View Attributes From Network** or right-click on

a port in the Resource Tree and select **Inventory -> View Attributes From Network**.

6. To view details for an interface, expand the port on which the interface resides in the Resource Tree (and expand further to reach a lower level, if necessary) and do one of the following:
  - Click the interface in the Resource Tree then click the **Details** tab.
  - To view details in a new window, right-click the interface in the Resource Tree and select **Inventory -> Details**. The system displays the details in a new window.



Details for an interface include the name, trace information, far-end interface information, and protection information. Protection information includes:

- Protection Type — the type of protection for the cross-connect, for example, Linear 1+1 or UPSR
- Protection Role and Direction — the member's protection role and, where applicable (UPSR and BLSR), the ring direction, for example, "Protecting, West"
- Protection Group Members — other members of the protection group, excluding the one for which details are shown

For Ethernet interfaces, additional information is shown if supported by the adapter, such as duplex mode and wire speed.

You can obtain interface attributes directly from the network instead of from the Nakina database and display them in a separate window. To do so, click the menu

arrow in the Details window and choose **View Attributes From Network** or right-click on an interface in the Resource Tree and select **Inventory -> View Attributes From Network**

For information about modifying interfaces, see “[Managing interfaces](#)” on page 104.

## 4.3 Update inventory in the Network Element View window

Use this procedure to update the NE inventory data in the Network Element View window. There are two options for updating the data:

- **Refresh Inventory of the Network Element:** updates the inventory data with the latest information from the Network Integrity database. The data will be current with the last Data Mining operation that was performed.
- **Resynchronize Inventory with the Network Element:** updates the alarms, equipment and interface inventory data with the latest information obtained directly from the network element.



Note: Inventory shows the provisioned view of a circuit pack. If a slot physically contains a circuit pack that is not provisioned, the slot will be reported as empty.

1. [“View shelf, circuit pack, port, and interface details” on page 48.](#)
2. Update the inventory by doing one of the following:
  - To update the inventory data with the latest information from the Network Integrity database, click **Refresh Inventory of the Network Element**.
  - To update the inventory data with the latest information directly from the network element, click **Resynchronize Inventory with the Network Element**.

Note: This option is not available if the NE is out of contact.



# 5 Configuring equipment

The Equipment Configuration window allows operators to view and set values for attributes on network elements, shelves, circuit packs, slots, ports, pluggable transceiver modules, and interfaces.

The actual resources and attributes that you can view or modify depend on the type of NE that you are working with, the resource type that you are working with, the permissions that you have been assigned and the commands that the adapter supports.

Consult your system administrator for more information.

This section explains how to:

- “View equipment configuration information” on page 53
- “Modify equipment configuration” on page 55
- “Refresh equipment configuration information” on page 57



**Note:** If while using the NOC you do not see menu items, tabs or buttons that are described in this documentation, it is because the Network Integrity administrator has not assigned the permission to your user account, or the feature has not been installed.

## 5.1 View equipment configuration information

Use this procedure to open the Equipment Configuration window and view the existing configuration information for an NE or for a specific resource on the NE.

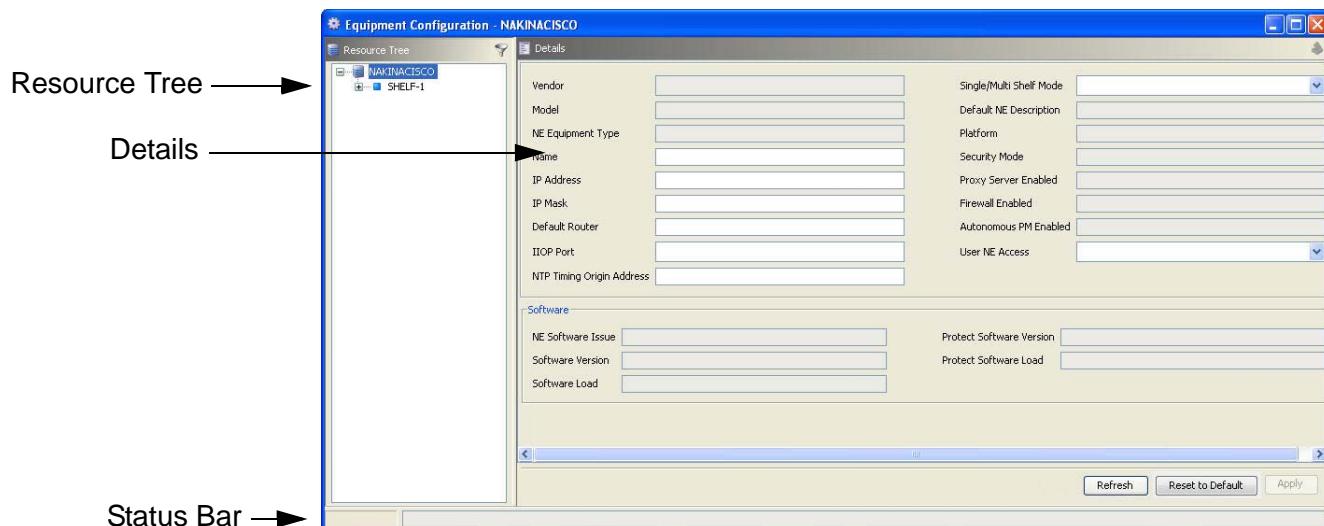
1. To view equipment configuration for an NE, do one of the following:
  - a. In the main window of the NOC, right-click the NE in the Topology view or Network Elements table and select **Provisioning > Equipment Configuration**.
  - b. In the Network Element View window, right-click the NE and select **Provisioning > Equipment Configuration** (see “[Viewing shelf level graphics](#)” on page 42 for more information about the Network Element View).

**Note:** You can also launch the Equipment Configuration window by right-clicking a shelf, slot, circuit pack, port, or interface in the Network Element View window and choosing **Provisioning > Equipment Configuration** (see “[View shelf, circuit pack, port, and interface details](#)” on page 48 for more information). In this case, the Equipment Configuration window opens with the Network Element field completed, as well as other resource-appropriate information.

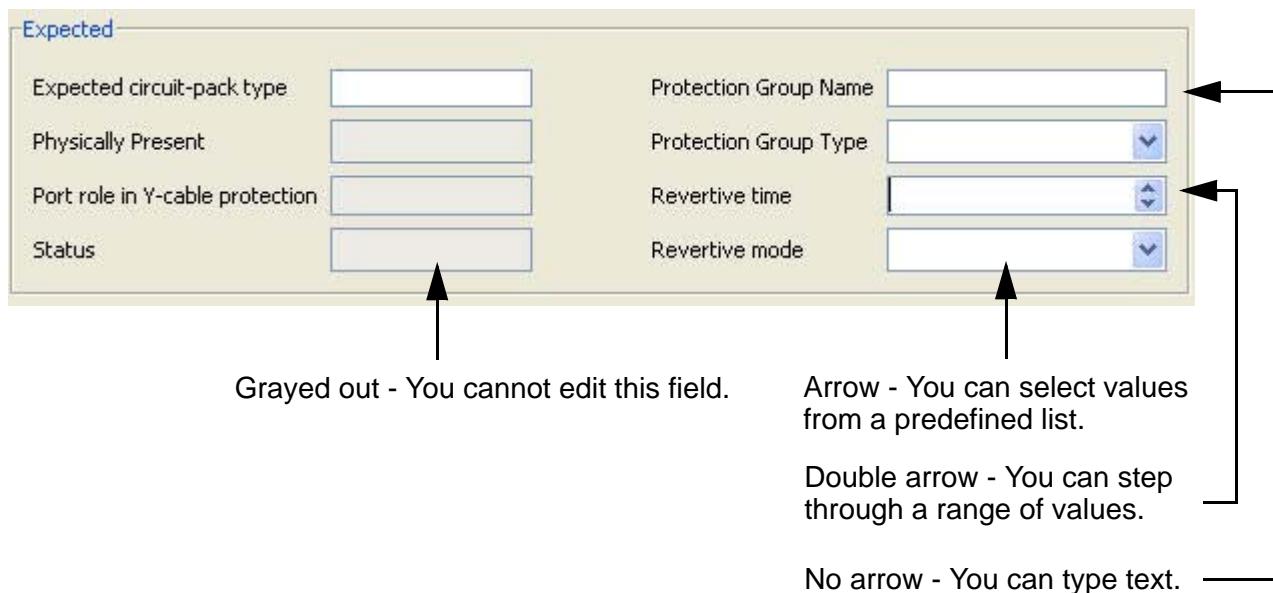
The Equipment Configuration window opens. The window has three sections:

- Resource Tree — The Resource Tree functions the same way as the Network Element View resource tree. See “[About the Resource Tree](#)” on page 46.
- Details — shows the details for the selected resource. The details that are shown are dependent on the adapter.

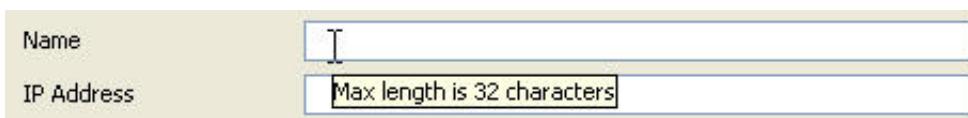
- Status Bar — shows the status of the Refresh, Reset to Default, or Apply operation, displays a message if the NE is out of contact, and shows the last Refresh time if a refresh has been performed.



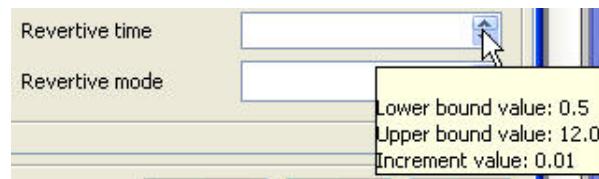
There are several field types that may be displayed, as shown in the following example.



You can view details about the attributes by moving the mouse over the label. For example:



Additional information may also be available about the valid values for the field. You can view this information by moving the mouse over the field. For example:



## 5.2 Modify equipment configuration

You can only modify equipment attributes if you have permission to do so. If you do not have permission to modify the attributes on a resource, the attributes are grayed out and only the Refresh button is available, not Apply or Reset to Default.

Some attributes cannot be modified even if you have permission to modify the resource. These attributes are grayed out.



**Note:** You can only modify attributes on NEs that are in contact. For out of contact NEs, the Equipment Configuration menu item is grayed out.

1. [View equipment configuration information.](#)
2. In the Resource Tree, navigate to the resource that you want to modify.

The Details panel for the resource is displayed. The information that is displayed depends on the resource. It is grouped into sections that are defined by the adapter.

A screenshot of the 'Equipment Configuration - NAKINACISCO' window. The left pane shows a 'Resource Tree' with a single node 'NAKINACISCO'. The right pane is titled 'Details' and contains two sections: 'Vendor' and 'Software'. The 'Vendor' section includes fields for Model, NE Equipment Type, Name, IP Address, IP Mask, Default Router, IIOP Port, and NTP Timing Origin Address. The 'Software' section includes fields for NE Software Issue, Software Version, Software Load, Protect Software Version, and Protect Software Load. At the bottom of the window are buttons for Refresh, Reset to Default, and Apply.

3. Click **Refresh** to display the current values.
4. In the **Details** section, modify the attributes as required.

You can move the mouse over an attribute for additional details, including whether the attribute is traffic affecting, dependencies, and valid values (valid values are only available if provided by the adapter).

Name	<input type="text"/>
IP Address	Max length is 32 characters

Fields may accept strings, integers, or may provide pull-down lists, depending on the attribute.

After you modify a attribute, it is shown in bold to indicate that it has changed.

If you type an incorrect value (for example, an incorrectly formatted IP address), it is shown in red italic text. It changes to regular text when you correct it.

If you modify a attribute on which another attribute depends, the dependent attribute is shown with a line through it, indicating that it is no longer valid.

Note: If you move to another resource in the Resource Tree without applying changes, a warning message is displayed asking if you want to discard your changes. Click OK to discard your changes or close the warning and then click Apply to apply them.

5. **Click **Apply**.**

Note: **Apply** is grayed out until you modify at least one attribute.

After you click **Apply**:

- The system validates all modified values before applying them to the NE and returns an error if a value is not valid.
- Modified attributes are no longer shown in a highlighted font.

6. If you want to reset all attributes to their default values, do the following:

a. **Click **Reset to Default**.**

Note: To perform a Reset to Default, you may need to remove the resource from service. If this is the case, an information message is displayed informing you of this. See “[Remove resources from service and return them to service](#)” on page 85 for more information.

Note: You can only reset values to defaults if you have the appropriate permission.

A warning message is displayed indicating that modifying parameters may affect traffic/service and asking if you want to proceed. You can click Yes to proceed or No to cancel.

b. **Click **Yes**.**

All attributes are reset to their default values on the screen only. They are not reset on the NE until you click **Apply**.

Note: Clicking on Reset to Default only resets the fields that have default values. If you have modified fields that have default values as well as fields that do not have default values, fields that do not have default values will remain as they are. They are not cleared.

c. **Click **Apply**.**

If there are any failures, all values are rolled back to what they were before the reset. An error dialog message is displayed to inform you of the problem.

## 5.3 Refresh equipment configuration information

When you refresh equipment configuration, the adapter retrieves all attributes from the NE for the resource that you currently have selected. For example, if you currently have a port selected, clicking Refresh will retrieve all attributes for that port.

1. In the **Equipment Configuration** window, click **Refresh**.

The system retrieves all attributes for the selected resources. If the operation fails, an error message is displayed indicating the cause of the failure.

## 6 Monitoring the network for alarms

---

The NI-Director Operations Console (NOC) provides a graphical, color-coded view of all the active alarms in the network. The color coding provides a quick assessment of the condition of any given NE in the Topology view and indicates the highest severity alarm condition. The NOC allows network operators to acknowledge and comment on the alarms so that other operators can see that the condition is being attended to. When the NE alarm condition is cleared, the alarm is cleared automatically from the NOC.

This section contains the following procedures for using the NOC to monitor the network alarm information:

- “[Understanding alarm colors and values](#)” on page 59
- “[Assess the overall alarm status of the network](#)” on page 60
- “[Information provided for individual alarms](#)” on page 61
- “[View and manage alarms in the entire network](#)” on page 62
- “[View and manage alarms in a group](#)” on page 67
- “[View and manage alarms for one network element](#)” on page 71
- “[Dynamically filter alarm data](#)” on page 73
- “[Search for alarms](#)” on page 74
- “[Turn dynamic alarm notification on or off](#)” on page 75
- “[View and manage circuit pack alarms](#)” on page 76
- “[Acknowledge an active alarm](#)” on page 77
- “[Add comments to an active alarm](#)” on page 78
- “[Manually refresh alarm data](#)” on page 78
- “[Manually resynchronize alarms with the NE](#)” on page 79

If you installed the Historical Event Viewer plugin, you can also view historic alarms, threshold crossing alarms (TCAs), and other events. See “[Viewing historic alarms, TCAs and other events](#)” on page 80.

To perform additional tasks that apply to all tables of data, such as alarms, see the following procedures:

- “[Sort table data](#)” on page 21
- “[Add or remove columns in a table](#)” on page 22
- “[Rearrange the columns in a table](#)” on page 23
- “[Save the visible table data to a file](#)” on page 24



Note: If while using the NOC you do not see menu items, tabs or buttons that are described in this documentation, it is because the Network Integrity administrator has not assigned the permission to your user account, or the feature has not been installed.

## 6.1 Understanding alarm colors and values

Alarm status is shown in the following locations:

- groups navigation tree
- topology view
- shelf level graphics



**Note:** The default alarm colors in Network Integrity are as follows: Red-Critical, Orange-Major, Yellow-Minor, Warning-White.

Each icon for a group, NE, or circuit pack provides one or more of the following elements that summarize its alarms status (depending on the location of the icon):

- main body color — indicates the highest severity alarm that has not been acknowledged on the device
- alarm balloon — provides details about the number of highest severity alarms that have not been acknowledged
- colored border — if present, indicates the highest severity of alarm that has been acknowledged, but still exists on the device.
- number in the center of the NE icon — indicates the total number of highest severity alarms (both acknowledged and unacknowledged) on the NE.

You can move your mouse over the number to see a text version of this information, for example, “New: 4 Minor Outstanding: 5 Minor”. “Outstanding” refers to unacknowledged alarms.

If the alarm balloon and the number in the center are the same (or the number of “New” alarms is equal to the number of “Outstanding” alarms), it means that no alarms have been acknowledged.

- number in the alarm balloon — indicates the most severe unacknowledged alarm count and severity on the NE.

You can move your mouse over the alarm balloon to see a summary of the alarms, for example, “New: 5 Major, 2 Minor”.

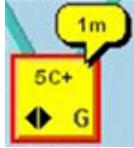
- letter **C** — indicates Critical alarms
- uppercase **M** — indicates Major alarms
- lowercase **m** — indicates Minor or Warning alarms
- plus sign (+) — indicates additional lower severity alarms.

If the plus sign is in the alarm balloon, there are additional lower severity alarms that have not been acknowledged. If the plus sign is in the center of the NE icon, there are additional lower severity alarms that have been acknowledged.

You can move your mouse over the alarm balloon to see a summary of the alarms

[“Sample NE and circuit pack alarm conditions” on page 60](#) shows several example alarm conditions and how to interpret them.

**Table 6–1: Sample NE and circuit pack alarm conditions**

Sample alarm condition	Meaning
	In this example, the overall color red (which may be different on your system) indicates that there are unacknowledged Critical alarms on the NE. In this example, because “5C+” appears in both the alarm balloon and the NE icon, it indicates that there are 5 Critical alarms plus other lower severity alarms, and none of them have been acknowledged.
	In this example, the color yellow (which may be different on your system) means that there are unacknowledged minor alarms on the NE. The red border indicates that there are acknowledged critical alarms on the NE. The “1m” in the alarm balloon indicates that there is one minor alarm that has not been acknowledged. The “5C+” indicates that there are 5 critical alarms plus other lower severity alarms in total on the NE.
	In this example, there is no alarm balloon, so all alarms have been acknowledged. The red border indicates that there are acknowledged critical alarms on the NE. The “5C+” indicates that there are 5 critical alarms plus other lower severity alarms in total on the NE.
	No alarms In this example, a gray NE icon with no alarm count in the center indicates that the NE has no alarms.
	Loss of contact The light blue color indicates a loss of contact with the NE. If the NE has a colored border, it indicates the alarm severity on the NE before contact was lost.
	Alarm monitoring is disabled “NR” indicates that alarm monitoring is disabled (Not Reported) for this NE. Alarm monitoring is controlled from the Network Integrity Fault Manager application. When alarm monitoring is enabled in the Network Integrity Framework, the NE alarm count is updated.

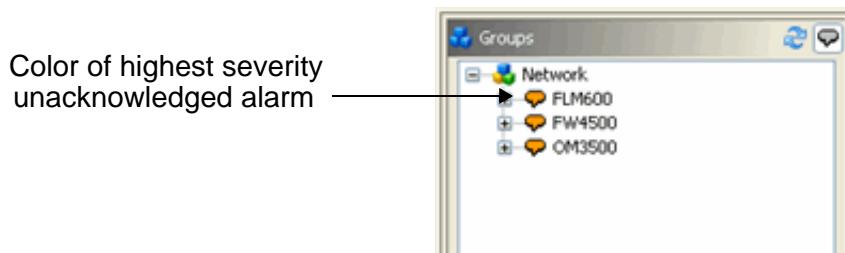
## 6.2 Assess the overall alarm status of the network

Use this procedure to quickly assess the overall alarm status of the entire network by looking for alarm balloons in the navigation tree.

If there is an alarm condition anywhere within a group, the highest level severity is indicated by the color of the balloon. This allows you to quickly scan the tree view and identify problems and then drill down to locate the source.

1. [“Log in” on page 8.](#)
2. If the alarm balloons are not displayed in the groups navigation tree, click the Show Alarms in Tree icon (see [“Use the groups navigation tree” on page 14](#) for more information).

An alarm balloon indicates a problem on an NE somewhere within the group, as shown in [“Interpreting network alarms” on page 61.](#)

**Figure 6–1: Interpreting network alarms**

**Note:** If your NOC role is not assigned to the groups that make up a container, the container may indicate an alarm severity that corresponds to an NE that is in a group that you are not authorized to access.

3. If an alarm balloon is present in the navigation tree for a group, select the group to display the Topology view and locate the source NE, or see “[View and manage alarms in a group](#)” on page 67 to obtain more details.

## 6.3 Information provided for individual alarms

Alarms can be displayed several different contexts. You can view

- all alarms in the network (described in “[View and manage alarms in the entire network](#)” on page 62)
- all alarms in a group (described in “[View and manage alarms in a group](#)” on page 67)
- all alarms on an NE (described in “[View and manage alarms for one network element](#)” on page 71)
- all alarms on a circuit pack (described in “[View and manage circuit pack alarms](#)” on page 76)

In each case, the information provided for individual alarms is the same, as described in the following table.

**Table 6–2: Information provided for individual alarms**

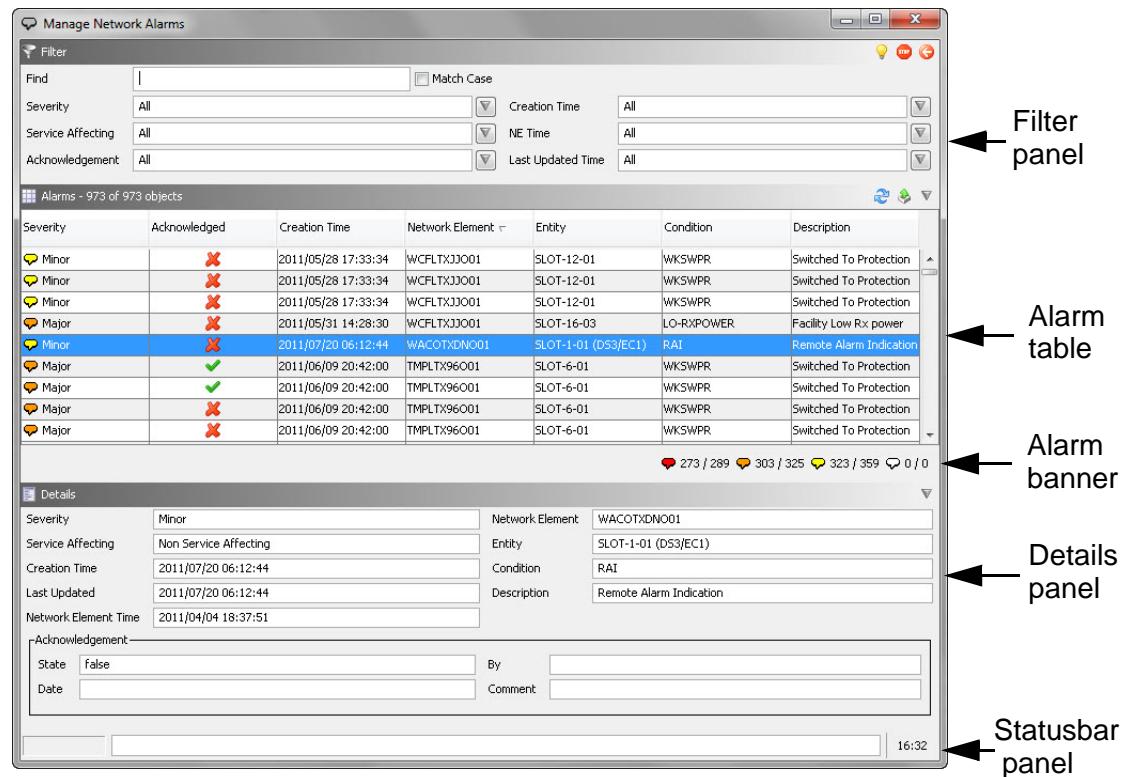
Column	Displayed by default	Description
Severity	Yes	The severity of the alarm. By default, this is one of: <ul style="list-style-type: none"> <li>• Critical</li> <li>• Major</li> <li>• Minor</li> <li>• Warning</li> </ul>
Service Affecting	No	Whether the alarm has an impact on the service being provided. If the alarm is service affecting, “SA” is shown in this column.
Acknowledged	Yes	Whether the alarm has been acknowledged. A green check box indicates that it has been acknowledged. A red X indicates that it has not been acknowledged.

Column	Displayed by default	Description
Creation Time	Yes	The time that the alarm was created in NOC.
Network Element	Yes	The network element on which the alarm occurred.
Entity	Yes	The component on the network element that generated the alarm.
Condition	Yes	A summary what caused the alarm.
Description	Yes	Additional information about the circumstances of the alarm, if applicable.
Acknowledged By	No	If acknowledged, the user ID that acknowledged the alarm.
Acknowledged Date	No	If acknowledged, the date that the alarm was acknowledged.
Acknowledged Comment	No	Any comments that users have entered or updated for acknowledged alarms.
Last Updated	No	The last time the alarm was updated on the NE.
Network Element Time	No	The time on the NE that the alarm was generated.

## 6.4 View and manage alarms in the entire network

Use this procedure to view and manage all of the alarms present in the network. Viewing and managing the alarms in the network is done using the Manage Network Alarms window.

The following graphic shows the panels of the Manage Network Alarms window.

**Figure 6–2: Manage Network Alarms window panels**

By default, when you first open the Manage Network Alarms window, only the Details panel is shown. The Details panel is always displayed. You can choose whether to display the other four panels. If you choose to display additional panels, the same panels will be displayed the next time you open the Manage Network Alarms window.

The following table summarizes the content of each panel.

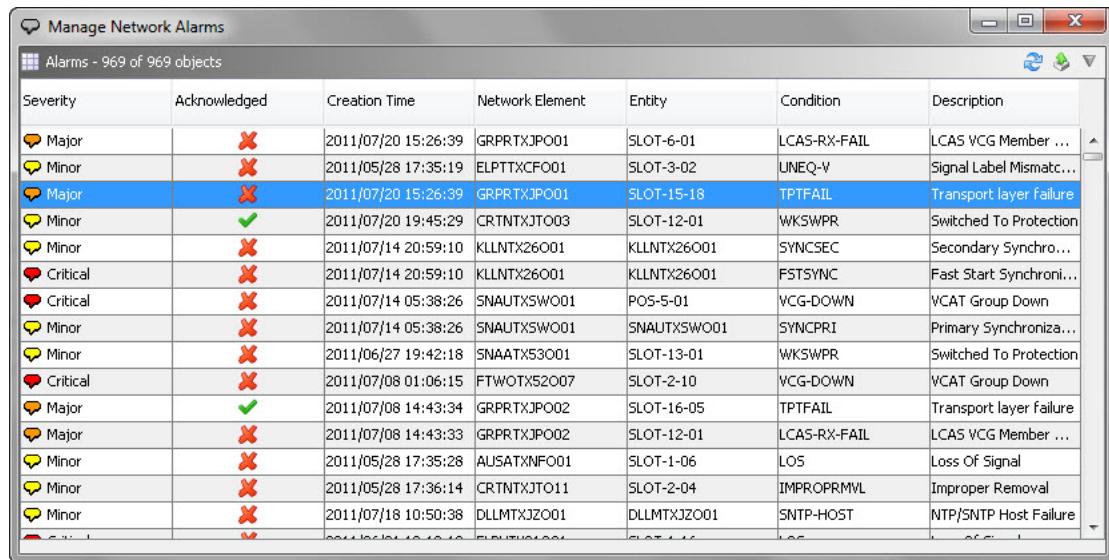
**Table 6–3: Descriptions of panels in the Manage Network Alarms window**

Panel	Description
Filter panel	Allows you display a subset of alarms in the network based on a variety of criteria. See “ <a href="#">Filter alarms in the Manage Network Alarms window</a> ” on page 66.
Alarm table	Detailed information about the alarms in the network.
Alarm banner	A summary of the current alarm count for the network. There are four alarm balloon colors, which represent the severity from highest to lowest (from left to right: Critical, Major, Minor and Warning.) For each severity there is a pair of numbers “x/y”, where x is the number of unacknowledged alarms of that severity in the network, and y is the total number of alarms of that severity in the network.
Details panel	Details about the selected alarm. If you select multiple alarms, nothing is displayed in this panel.

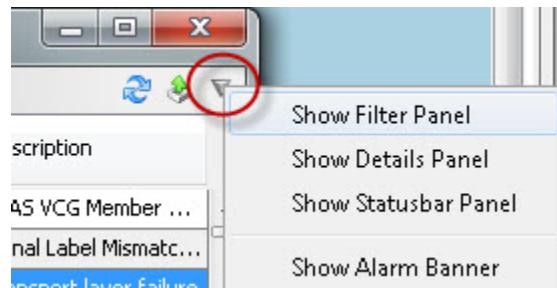
Panel	Description
Statusbar panel	Contains a progress bar, status text, and a clock. The progress bar and status text are activated when the alarms are being retrieved from the server and deactivated when the alarms are all retrieved.

- From the NOC main menu, choose **Surveillance > Manage Alarms**.

The Manage Network Alarms window opens. The panels that are displayed are the same ones that were displayed when you last accessed the window. The alarm table is always displayed.

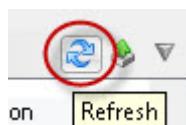


- To display additional panels, or to remove panels from the display, click the menu arrow and choose the option to display or hide.

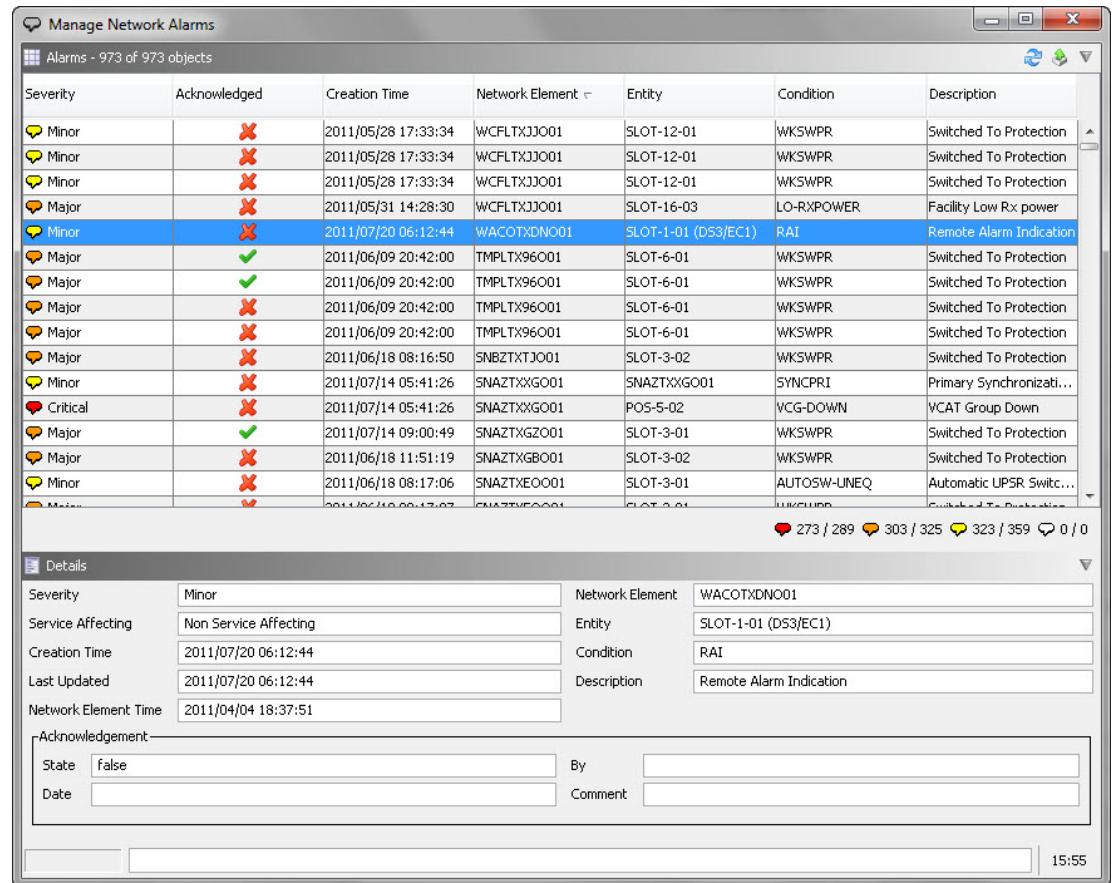


For details about the panels, see “Manage Network Alarms window panels” on page 63 and “Descriptions of panels in the Manage Network Alarms window” on page 63.

- To manually refresh alarm data (and topology data) with the latest information from the Network Integrity database, click the Refresh button.



4. If you want to view a subset of the alarms in the network, you can “[Filter alarms in the Manage Network Alarms window](#)” on page 66.
5. To view details about an alarm, do the following:
  - a. Display the **Details** panel by clicking the menu arrow and choosing **Show Details Panel**.
  - b. Click the alarm to display details about the alarm in the **Details** section of the window, for example:



You can also right-click the alarm and select **Details** to display details about the alarm in a new window.

6. To view the alarm attributes, right-click on an alarm in the list and select **View Attributes from Network** from the pop-up menu.  
The network alarm attributes are displayed.
7. To acknowledge an alarm, see “[Acknowledge an active alarm](#)” on page 77.  
If you want to acknowledge multiple alarms at the same time, use **Shift-click** or **Ctrl-click** to select them.
8. To add comments to an active alarm, see “[Add comments to an active alarm](#)” on page 78.  
If you want to add the same comment to multiple alarms at the same time, use **Shift-click** or **Ctrl-click** to select them.

9. In the alarm table, you can also
  - “Sort table data” on page 21
  - “Add or remove columns in a table” on page 22
  - “Rearrange the columns in a table” on page 23
  - “Save the visible table data to a file” on page 24 (Note that when data is exported from the Alarm view, the system exports the currently visible rows and columns of alarms.)

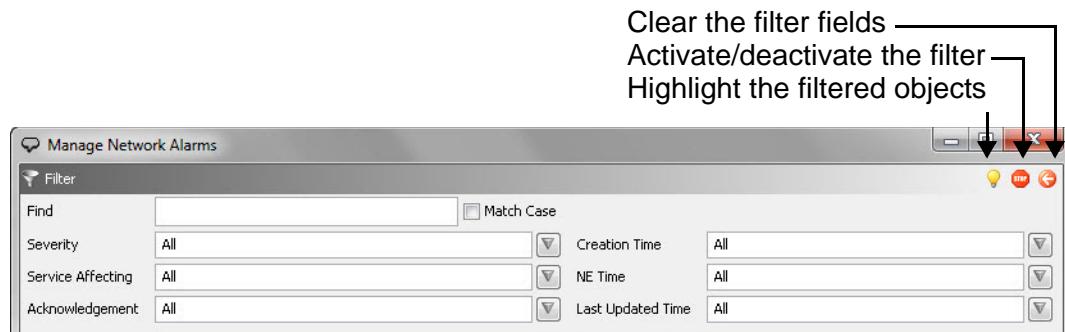
#### 6.4.1 Filter alarms in the Manage Network Alarms window

Use this procedure to filter the information in the alarms table. For example, you can choose to view only critical or service-affecting alarms.

As you select the filter criteria, the list will update to display the entries that match the filter. You can also activate highlighting which will highlight the filtered entries. See “Highlight entries in a filtered table” on page 20.

1. Display the **Filter** panel by clicking the menu arrow and choosing **Show Filter Panel**.

The Filter panel is displayed, for example:



In this example, you can highlight the filtered objects, activate and deactivate the filter, and clear the filter fields. See “Use the Network Elements table” on page 16 for more information.

2. Enter the search criteria in the **Find** field, and select the **Match Case** check box if you want to consider the case in the search.

For example, if you wanted to see entries containing the word “link”, type “link” in the Find field.

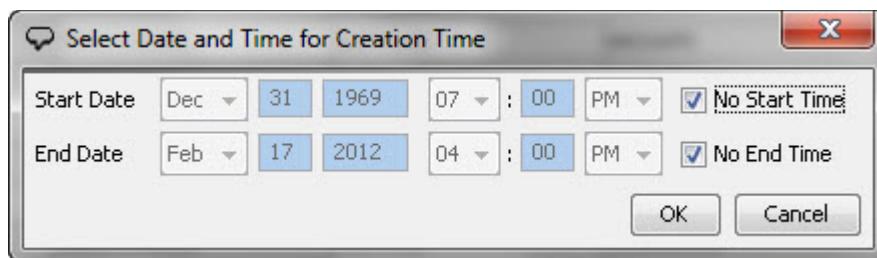
As you type in the Find field, the alarms table is dynamically updated with the alarms that match the typed criteria.

You can also leave this field blank (if, for example, you wanted to search for all critical alarms regardless of name).

3. To search for alarms of a specific severity, select the severity from the **Severity** pull-down list.
4. To search for alarms based on whether they are service affecting, select one of the following from the **Service Affecting** pull-down list:

- All — The alarms are not filtered based on whether they are service affecting.
  - True — Only alarms that are service affecting will be displayed.
  - False — Only alarms that are not service affecting will be displayed.
5. To search for alarms based on whether or not they have been acknowledged, select one of the following from the **Acknowledgement** pull-down list:
    - All — The alarms are not filtered based on whether they are acknowledged.
    - True — Only alarms that are acknowledged will be displayed.
    - False — Only alarms that are not acknowledged will be displayed.
  6. To search for alarms based on Creation Time, NE Time, or Last Updated time, do the following:
    - a. Click the associated arrow and choose **Set**.

The Select Date and Time dialog box is displayed, for example:



By default, the range is set to no start or end time.

- b. If you want to specify a start time, clear the **No Start Time** check box and in the **Start Date** fields, specify the beginning of the time period in which to search.
- c. If you want to specify an end time, clear the **No End Time** check box and in the **End Date** fields, specify the end of the time period in which to search.

**Note:** When you define a start and end time, the system uses the local time setting on your computer, not the current time displayed in the NOC. The historical events will be retrieved and displayed based on the local time setting on your computer, so make sure to offset the start and end times according to your time zone offset.

- d. Click **OK**.

7. To turn off filtering, click the **Activate/Deactivate the Filter** button.

## 6.5 View and manage alarms in a group

Use this procedure to quickly assess the overall alarm status of a group (static, dynamic, or container).

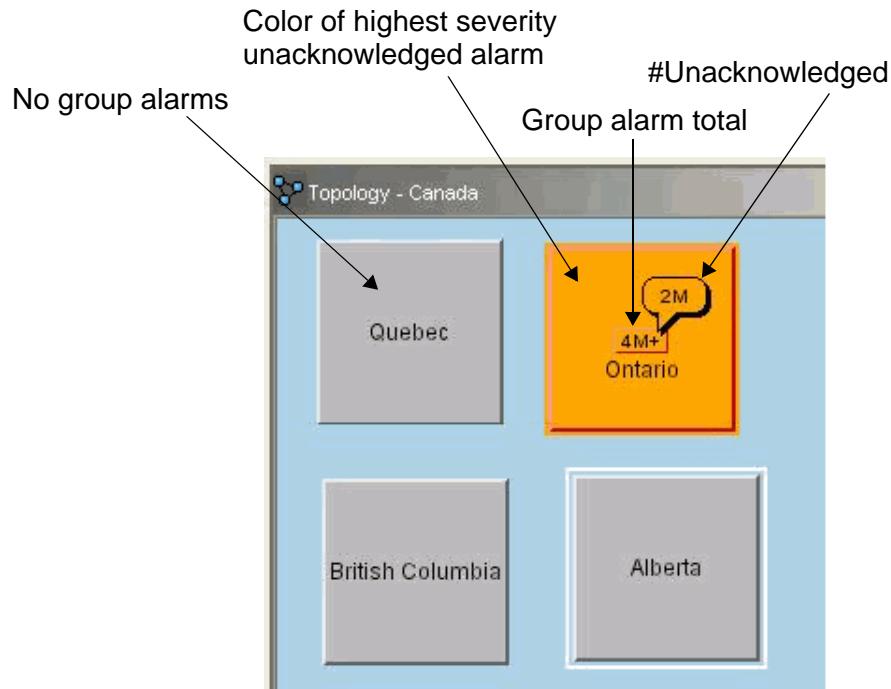
When you select a container group in the navigation tree, the NOC displays a status summary of the contained groups in the Topology area.

The color of the alarm balloon or the color of the group summary indicates the highest severity of unacknowledged alarms on the NEs in the group. The number in the center

of the group summary indicates the total number of the highest severity alarms in the group, and the alarm balloon indicates the highest severity of unacknowledged alarms.

1. To display the overall status of a container group, click on a container group in the groups navigation tree.

The system displays the alarm summary for each of the contained groups in the Topology view, as shown in the following example.



2. To view the alarms for all NEs in an NE group (static, dynamic, or container), do one of the following:

- Select the NE group in the groups navigation tree and click the **Group Alarms** tab.

A list of alarms for the NEs in the NE group is displayed in the Group Alarms tab under the Topology window.

A summary of the current alarm count for all NEs in the selected group appears at the bottom right of the alarm panel. There are four alarm balloon colors, which represent the severity from highest to lowest (from left to right: critical, major, minor and warning.) For each severity there is a pair of numbers "x/y", where x is the number of unacknowledged alarms of that severity in the network, and y is the total number of alarms of that severity in the network. If you have clicked on the top-level group, typically called "Network", the values all read "-/-".

If a green check box is displayed in the "Acknowledged" column, the alarm condition has been acknowledged. If there is no check box, the alarm has not been acknowledged. In this case, you can "[Acknowledge an active alarm](#)" on page 77.

- Right-click the NE group in the groups navigation tree or the Topology view and choose **Surveillance > Manage Alarms**.

The list of alarms in the group opens in a new window, similar to the following:

Severity	Acknowledged	Creation Time	Network Element	Entity	Condition	Description
Major	X	2010/01/20 17:3...	OM3500-1-SP	DS1-4 Port 11	\\"DS1 Rx Loss Of...	\\"DS1 Rx Loss Of...
Major	X	2010/01/20 16:4...	OM3500-1-SP	SP-13	Loss Of Shelf Pri...	Loss Of Shelf Pri...
Critical	X	2010/01/20 16:4...	OM3500-1-SP	Fan-2	Fan Missing	Fan Missing
Major	X	2010/01/20 16:4...	OM3500-1-SP	OM3500-1-SP	ST5 Rx Loss Of P...	ST5 Rx Loss Of P...
Minor	X	2010/01/20 16:4...	OM3500-1-SP	OC12-10 Port 1	SDCC Link Failure	OC12 Rx Signal ...
Major	X	2010/01/20 17:3...	OM3500-1-SP	DS1-4 Port 6	\\"DS1 Rx Loss Of...	\\"DS1 Rx Loss Of...
Minor	X	2010/01/20 16:4...	OM3500-1-SP	SP-3	Circuit Pack Missing	Circuit Pack Missing
Major	X	2010/01/20 16:4...	OM3500-1-SP	OM3500-1-SP	ST53C Rx Loss O...	ST53C Rx Loss O...
Minor	X	2010/01/20 16:4...	OM3500-1-SP	OM3500-1-SP	BITSin-A Rx Loss...	BITSin-A Rx Loss...
Major	X	2010/01/20 17:3...	OM3500-1-SP	DS1-4 Port 3	\\"DS1 Rx Loss Of...	\\"DS1 Rx Loss Of...

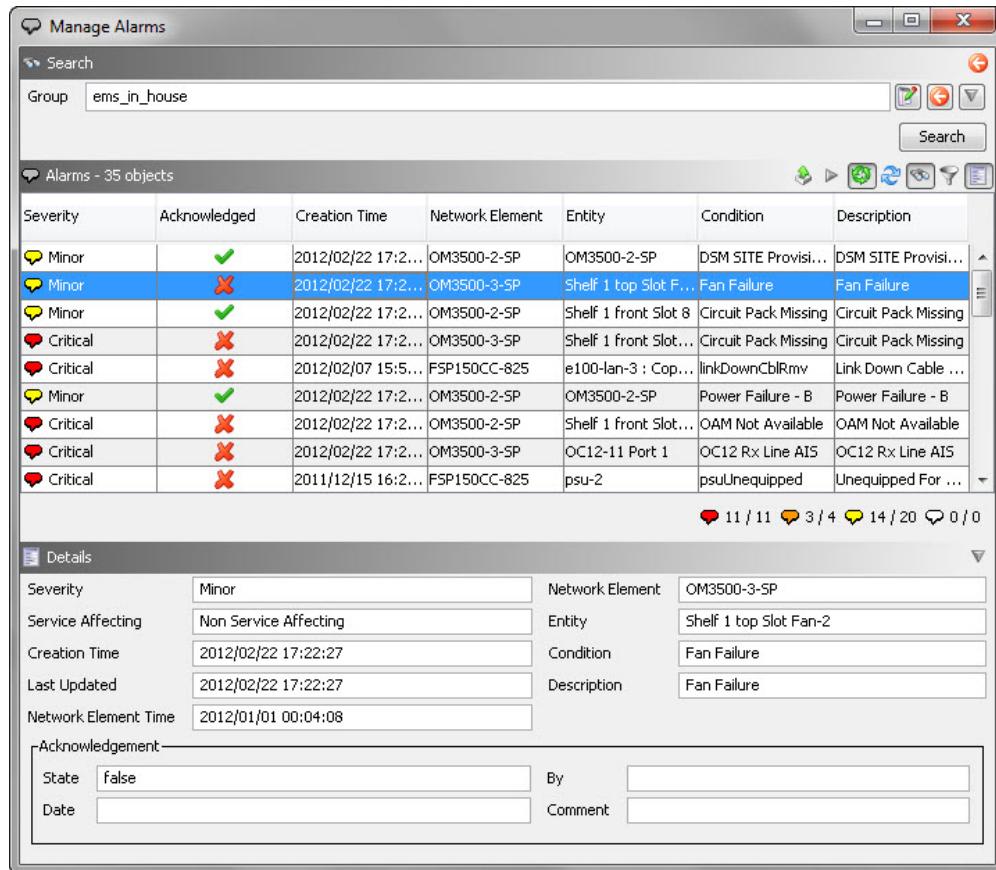
You can open the alarms table in a separate window by clicking the Detach button.



3. To view details about an alarm, do the following:
  - a. Click the **Show/Hide Details Panel** button to display the **Details** panel.



- b. Click the alarm to display details about the alarm in the Details section of the window, for example:



You can also right-click the alarm and select **Details** to display details about the alarm in a new window.

4. To view the alarm attributes, right-click on an alarm in the list and select **View Attributes from Network** from the pop-up menu.  
The network alarm attributes are displayed.
5. To search for alarms, see "[Search for alarms](#)" on page 74.
6. From the alarm table, you can perform the following tasks:
  - "[Acknowledge an active alarm](#)" on page 77
  - "[Add comments to an active alarm](#)" on page 78
  - "[Manually refresh alarm data](#)" on page 78
  - "[Manually resynchronize alarms with the NE](#)" on page 79
  - "[Sort table data](#)" on page 21
  - "[Add or remove columns in a table](#)" on page 22
  - "[Rearrange the columns in a table](#)" on page 23
  - "[Save the visible table data to a file](#)" on page 24
  - "[View and manage alarms for one network element](#)" on page 71

## 6.6 View and manage alarms for one network element

Use this procedure to view and manage the alarms for one network element (NE).



**Note:** The NOC displays NE alarm times according to the NOC user's local time zone setting, not according to the time where the NE is located. For example, if an NE on the west coast had an alarm at 3:00 PM PST (Pacific Standard Time), a NOC user on the east coast would see the alarm displayed as 6:00 PM EST (Eastern Standard Time).

1. In the Network Elements table or the Topology view, click the NE for which to view alarms.
2. Right-click and select **Surveillance > Manage Alarms** from the pop-up menu.

The alarms for the NE are displayed, similar to the following example:

The screenshot shows a Windows application window titled "Manage Alarms". At the top, there is a search bar with the text "Network Element: OM3500-2-SP" and a "Search" button. Below the search bar is a toolbar with various icons. The main area is a table titled "Alarms - 17 objects". The table has columns: Severity, Acknowledged, Creation Time, Network Element, Entity, Condition, and Description. The data in the table is as follows:

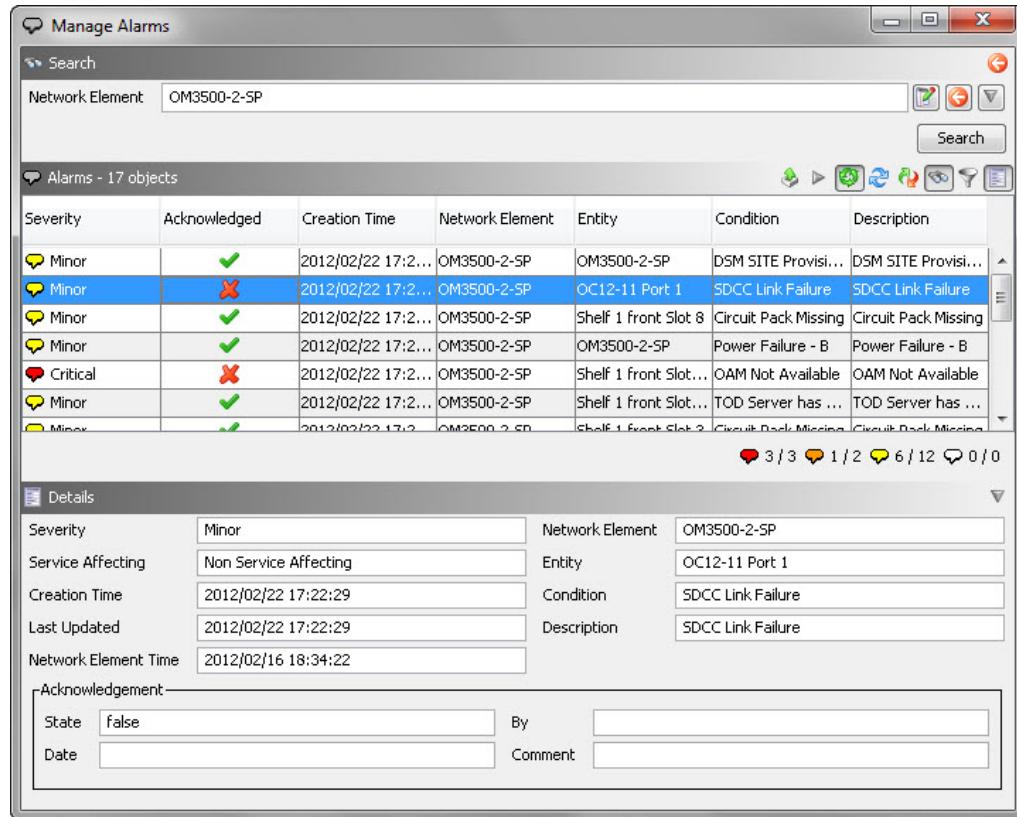
Severity	Acknowledged	Creation Time	Network Element	Entity	Condition	Description
Major	✗	2010/01/20 17:2...	OM3500-2-SP	DS1-7 Port 11	DS1 Rx Loss Of 5...	DS1 Rx Loss Of ...
Major	✗	2010/01/20 17:2...	OM3500-2-SP	DS1-7 Port 10	DS1 Rx Loss Of 5...	DS1 Rx Loss Of ...
Major	✗	2010/01/20 17:2...	OM3500-2-SP	DS1-7 Port 4	DS1 Rx Loss Of 5...	DS1 Rx Loss Of ...
Major	✗	2010/01/20 17:2...	OM3500-2-SP	DS1-7 Port 1	DS1 Rx Loss Of 5...	DS1 Rx Loss Of ...
Major	✗	2010/01/20 17:2...	OM3500-2-SP	DS1-7 Port 2	DS1 Rx Loss Of 5...	DS1 Rx Loss Of ...
Minor	✗	2010/01/20 17:2...	OM3500-2-SP	OC12-11 Port 1	SDCC Link Failure	SDCC Link Failure
Major	✓	2010/01/20 17:2...	OM3500-2-SP	DS1-7 Port 9	DS1 Rx Loss Of 5...	DS1 Rx Loss Of ...
Minor	✗	2010/01/20 20:3...	OM3500-2-SP	OC12-12 Port 1	\\"STS Rx Unequi...	\\"STS Rx Unequi...
Major	✗	2010/01/20 17:2...	OM3500-2-SP	DS1-7 Port 3	DS1 Rx Loss Of 5...	DS1 Rx Loss Of ...
Major	✗	2010/01/20 17:2...	OM3500-2-SP	DS1-7 Port 5	DS1 Rx Loss Of 5...	DS1 Rx Loss Of ...

At the bottom of the window, there are several status indicators: 0 / 0, 12 / 13, 4 / 4, and 0 / 0.

- You can open the alarms table in a separate window by clicking the Detach button.
3. To view details about an alarm, do the following:
    - a. Click the **Show/Hide Details Panel** button to display the **Details** panel.



- b. Click the alarm to display details about the alarm in the Details section of the window, for example:



You can also right-click the alarm and select **Details** to display details about the alarm in a new window.

4. To view the alarm attributes, right-click on an alarm in the list and select **View Attributes from Network** from the pop-up menu.  
The network alarm attributes are displayed.
5. To close the attributes window, click **Cancel**.
6. To search for alarms, see “[Search for alarms](#)” on page 74.
7. From the alarm table, you can also perform the following tasks:
  - “[Acknowledge an active alarm](#)” on page 77
  - “[Add comments to an active alarm](#)” on page 78
  - “[Manually refresh alarm data](#)” on page 78
  - “[Manually resynchronize alarms with the NE](#)” on page 79
  - “[Sort table data](#)” on page 21
  - “[Add or remove columns in a table](#)” on page 22
  - “[Rearrange the columns in a table](#)” on page 23
  - “[Save the visible table data to a file](#)” on page 24 (Note that when data is exported from the Alarm view, the system exports the currently visible rows and columns of alarms.)

- “View and manage alarms for one network element” on page 71

## 6.7 Dynamically filter alarm data

Use this procedure to dynamically filter the information in the alarms table. For example, you can choose to view only critical or service-affecting alarms.



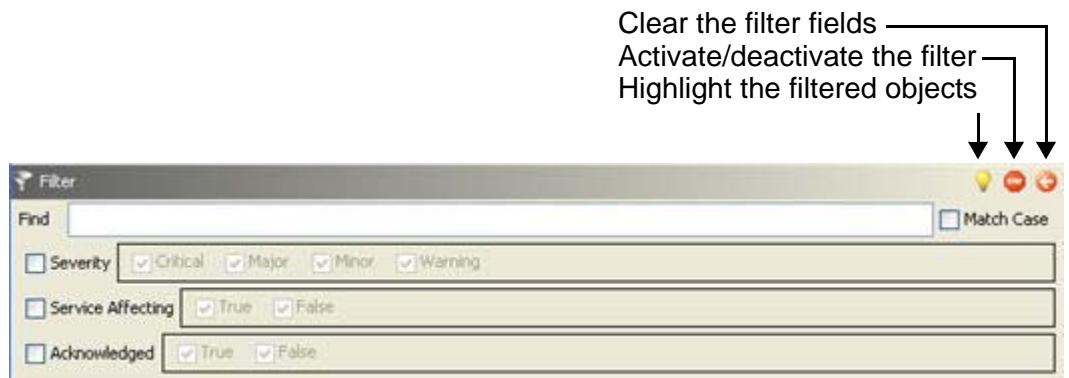
Note: This procedure also applies to other information tables.

As you select the filter criteria, the list will update to display the entries that match the filter. You can also activate highlighting which will highlight the filtered entries. See “Highlight entries in a filtered table” on page 20.

1. Click the **Show/Hide Filter Panel** icon.



The Filter panel is displayed, as in this alarm filter example.



In this example, you can highlight the filtered objects, activate and deactivate the filter, and clear the filter fields. See “Use the Network Elements table” on page 16 for more information.

2. Enter the search criteria in the **Find** field, and select the **Match Case** check box if you want to consider the case in the search.

For example, if you wanted to see entries containing the word “link”, type “link” in the **Find** field.

As you type in the Find field, the alarms table is dynamically updated with the alarms that match the typed criteria.

You can also leave this field blank (if, for example, you wanted to search for all critical alarms regardless of name).

3. To perform additional filtering, you can select check boxes for additional criteria, such as **Severity**, **Service Affecting**, or **Acknowledged**.

After you select the main check box, you can specify the conditions. For example, if you select the Severity check box, you can select the check boxes for the severities that you want to display.

The list will update dynamically as you select the search criteria.

Note: The Service Affecting column is not displayed in the alarms table by default. If you want to see the column, you must add it (see ["Add or remove columns in a table" on page 22](#)). This column displays "SA" if the alarm is service affecting. Otherwise, it is blank. For example:

Service Affecting
SA
SA
SA
SA

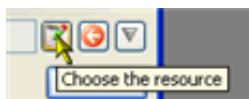
4. To turn off filtering, click the **Clear the Filter Fields** button.
5. To stop displaying the filter panel, click the **Show/Hide Filter Panel** icon again.

## 6.8 Search for alarms

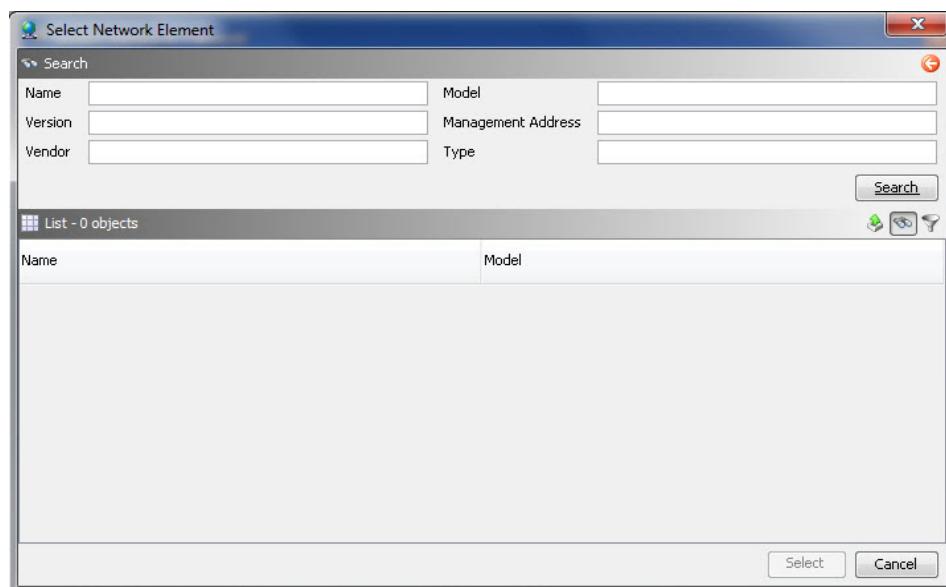
1. To search for alarms for an NE, do the following:
  - a. Click the **Choose a Resource Type** icon and choose **Network Element**.



- b. Click the **Choose the Resource** icon.



The Select the Network Element window opens.



- c. Type the search criteria in the fields provided and click **Search**.

To search for all NEs, leave the search fields blank and click Search.

Note: Search is underlined to show that no search has been performed using the currently defined criteria. If the results table is empty and Search is underlined, this indicates that no search has been performed. If the results table is empty and Search is not underlined, this indicates that the search has returned no results.

- d. Choose an NE in the **Network Elements** list and click **Select**, then click **Search** to update the alarms list for the new NE.

The alarms list is updated to show alarms for the NE.

2. To search for alarms for a group, do the following:

- a. Click the **Choose a Resource Type** icon and choose **Group**.
- b. Click the **Choose the Resource** icon.
- c. In the **Select Group** window, choose the group for which to display alarms, and click **Select**, then click **Search** to update the alarms list for the new group.

The alarms list is updated to show alarms for the group.

3. You can clear the resource field by clicking the **Clear the Resource** button.



## 6.9 Turn dynamic alarm notification on or off

Use this procedure to turn alarm notification on or off.



Note: By default, alarm notification is On.

For any list of alarms, the operator can turn alarm notification on or off by toggling the “Use Notifications” button on or off. When “Use Notifications” is on, the system displays the alarms as they are updated in the Network Integrity database. When “Use Notifications” is off, the system stops updating the list of alarms. Turning notification off can be useful if there is a flood of alarms and you want to stop the display of new alarms.

If “Use Notifications” is off, and you want to see the latest alarm data, you must perform a manual refresh. See “[Manually refresh alarm data](#)” on page 78.

1. To turn dynamic alarm notification on, in the Alarms section of the NOC window, click the **Use Notifications** button so that it is depressed/highlighted.



The system will display alarms as they become available in the Network Integrity database.

2. To turn dynamic alarm notification off, click the **Use Notifications** button so that it is not depressed/highlighted.

The system will stop displaying new alarms.

You can also turn dynamic alarm notifications on or off for individual NEs in the Manage Alarms window for the NE. See [“View and manage alarms for one network element” on page 71](#) for more information about the Manage Alarms window.

## 6.10 View and manage circuit pack alarms

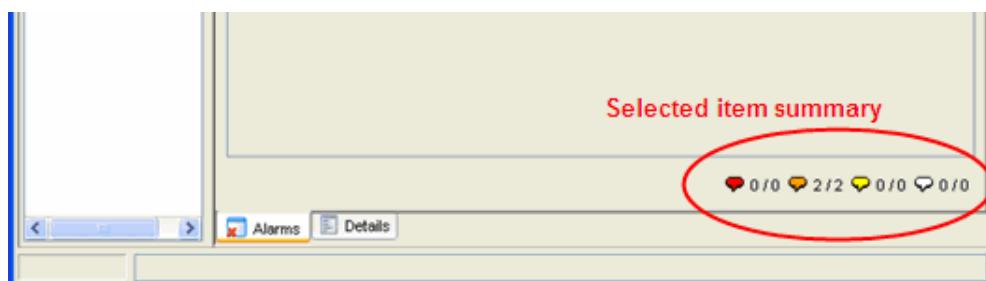
Use this procedure to view and manage circuit pack alarms.

1. In the Network Elements table or in the Topology view, click on the network element that contains the circuit packs you want to view.
2. Right-click the network element and select **Shelf Level Graphics**.

Alternatively, you can double-click an NE to open the shelf level graphics view. If the NE contains more than one shelf, click on a shelf in the Navigation Tree in the SLG window.

If a circuit pack in the shelf has an alarm condition, the circuit pack is color coded to indicate the severity. Examples are shown in [“Sample NE and circuit pack alarm conditions” on page 60](#).

The alarm summary at the bottom right of the window shows the alarm summary for the selected item. If the shelf is selected it is the alarm summary for the shelf. If a circuit pack is selected, it is the alarm summary for the circuit pack.



You can open the alarm list in a separate window by clicking the Detach button.



3. If the **Alarms** tab is selected, the alarm details for the selected item are displayed.
4. From this list you can perform the following actions:
  - [“Acknowledge an active alarm” on page 77](#)
  - [“Add comments to an active alarm” on page 78](#)
  - [“Manually refresh alarm data” on page 78](#)
  - [“Manually resynchronize alarms with the NE” on page 79](#)
  - [“Sort table data” on page 21](#)
  - [“Add or remove columns in a table” on page 22](#)

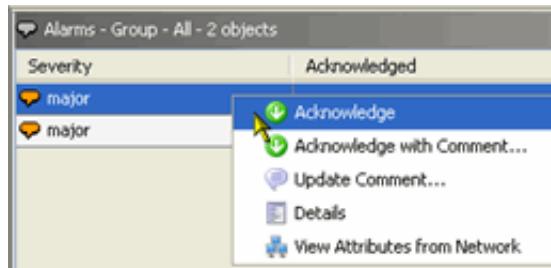
- “Rearrange the columns in a table” on page 23
- “Save the visible table data to a file” on page 24 (Note that when data is exported from the Alarm view, the system exports the currently visible rows and columns of alarms.)
- “View and manage alarms for one network element” on page 71

## 6.11 Acknowledge an active alarm

Use this procedure to acknowledge an active alarm so that other NOC operators can see that the condition is being attended to. This procedure also provides the option of acknowledging and commenting at the same time. If you just want to comment on an alarm, see “Add comments to an active alarm” on page 78.

When an alarm is acknowledged, it is still active in the system. If required, an acknowledged alarm can be toggled back to an unacknowledged state. For an explanation of how acknowledgement affects alarm the colors displayed by the NOC, see “Understanding alarm colors and values” on page 59.

1. Display the required list of alarms. See “View and manage alarms in a group” on page 67, “View and manage alarms for one network element” on page 71, or “View and manage circuit pack alarms” on page 76.  
Unacknowledged alarms are indicated by a red X in the Acknowledged column.
2. Right-click on the alarm to be acknowledged and select either **Acknowledge** or **Acknowledge with Comment** from the pop-up menu.



If you selected **Acknowledge**, the system displays a green check mark in the Acknowledged column, as shown in this example.

The screenshot shows a table titled "Alarms - 2 objects". The columns are "Severity" and "Acknowledged". There are two rows, both labeled "major". The "Acknowledged" column for the first row now has a green checkmark icon, indicating it is acknowledged. The "Acknowledged" column for the second row still has a red "X" icon, indicating it is not acknowledged.

Severity	Acknowledged
major	✓
major	✗

If you selected **Acknowledge with Comment** the system displays the Alarm Comment window.



3. Type the desired comment in the window, then click **Acknowledge**.
4. Right-click on the alarm to be acknowledged and select **Acknowledge** from the pop-up menu.

#### To remove the alarm acknowledgement

5. Right-click on the desired alarm and select **Unacknowledge** from the pop-up menu.
6. To add a comment to an alarm, see "[Add comments to an active alarm](#)" on page 78.

## 6.12 Add comments to an active alarm

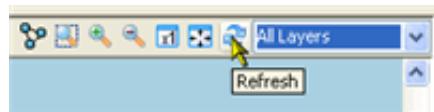
Use this procedure to add comments to an active alarm so that current troubleshooting actions can be communicated to other NOC users. For example, if a trouble ticket is raised, it can be communicated in the comment. At any time, any operator can update the comment associated with an active alarm or clear all comments from the alarm. To acknowledge and comment in one action, see "[Acknowledge an active alarm](#)" on page 77. You can also use this procedure to clear comments from an active alarm.

1. Display the required list of alarms. See "[View and manage alarms in a group](#)" on page 67, "[View and manage alarms for one network element](#)" on page 71, or "[View and manage circuit pack alarms](#)" on page 76.
2. Right-click on the alarm to be commented and select **Update Comment** from the pop-up menu.
3. In the comment window, type the desired comment.

## 6.13 Manually refresh alarm data

Use this procedure to manually refresh alarm data (and topology data) with the latest information from the Network Integrity database. If "Use Notifications" is turned off, this is the only way to refresh the alarm data. To turn on dynamic alarm notification, see "[Turn dynamic alarm notification on or off](#)" on page 75.

1. Click the **Refresh** icon.



## 6.14 Manually resynchronize alarms with the NE

Use this procedure to manually resynchronize alarm data with the latest information from the NE. This procedure clears the alarms in the Network Integrity database and retrieves them again from the NE.

1. Display the list of alarms for the NE or shelf. See “[View and manage alarms for one network element](#)” on page [71](#) or “[View and manage circuit pack alarms](#)” on page [76](#).
2. Click the **Resync** icon.



The alarm list is resynchronized with the NE.

## 7 Viewing historic alarms, TCAs and other events

The Network Integrity Framework can be configured to store historical events for Nakina managed NEs. If the administrator enabled the Historical Event Viewer plugin, you can view the event history for a selected NE.

Use this procedure to search for the following historic faults:

- historic alarms
- historic threshold crossing alarms (TCAs)
- historic other events

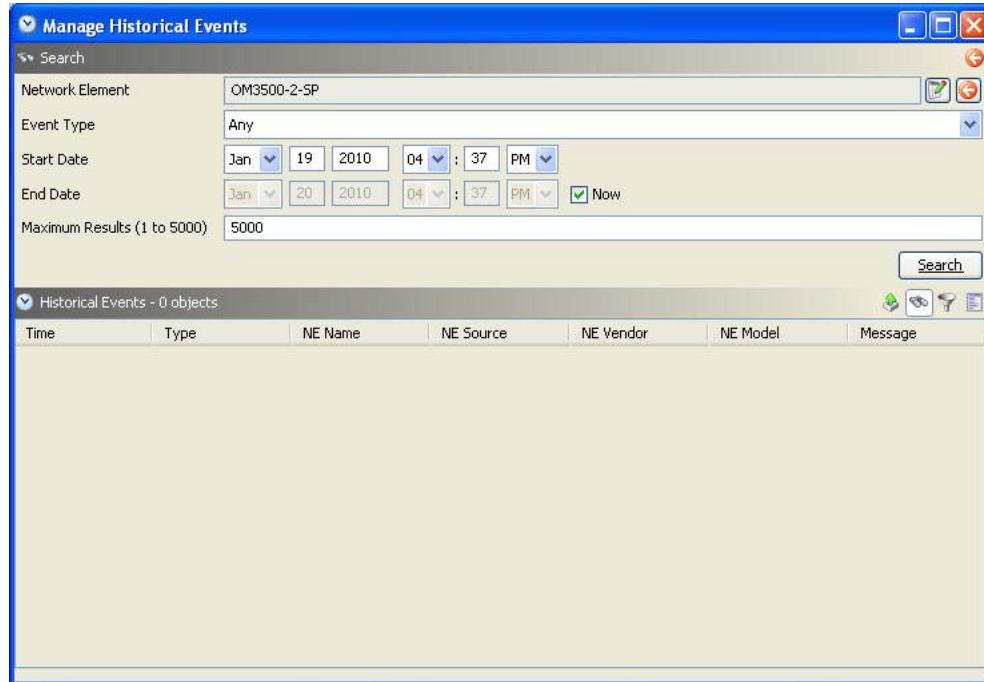


Note: TCAs and other events from Network Integrity R5 adapters are stored under "Historic Other" events in this release.

You can find historical events on the selected NE for any time period and you can view details about any item in the search results.

1. in the Network Elements table or in the Topology view, right-click the NE for which you want to view historical events and select **Surveillance > Manage Historical Events**.

The system displays the Manage Historical Events window.

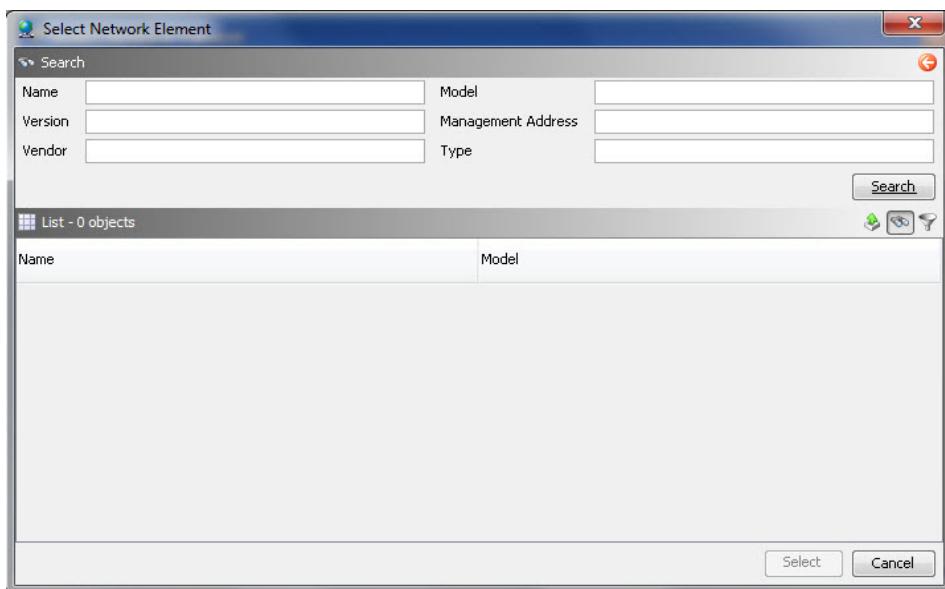


2. The **Network Element** field will contain the name of the NE that you selected.
3. If you want to change the NE, do the following:

- a. Click the **Choose the Resource** button.



The Select Network Element window opens.



- b. Type the search criteria in the fields provided and click **Search**.

To search for all NEs, leave the search fields blank and click Search.

**Note:** Search is underlined to show that no search has been performed using the currently defined criteria. If the results table is empty and Search is underlined, this indicates that no search has been performed. If the results table is empty and Search is not underlined, this indicates that the search has returned no results.

- c. Choose an NE in the **Network Elements** list and click **Select**.

The NOC places the selected NE name in the Network Element field.

4. From the **Historic Event Type** list select the type of historic event to search for: **Historic Alarms**, **Historic TCAs**, **Historic Other Events** or **All**.
5. In the **Start Date** and **End Date** fields, specify the beginning and ending period for the events you are interested in.

Select the **Now** check box to specify that the period ends now.

**Note:** When you define a start and end time, the system uses the local time setting on your computer, not the current time displayed in the NOC. The historical events will be retrieved and displayed based on the local time setting on your computer, so make sure to offset the start and end times according to your time zone offset.

6. In the **Maximum Results** field, specify the maximum number of results to display.
7. Click **Search** to display the historical events that match the search criteria.

The NOC displays the results, as shown in the following example:

The screenshot shows the 'Manage Historical Events' window. At the top, there is a search panel with fields for Network Element (OM3500-2-SP), Event Type (Any), Start Date (Jan 19, 2010, 04:37 PM), End Date (Jan 20, 2010, 04:46 PM, checked 'Now'), Maximum Results (5000), and a 'Search' button. Below the search panel is a table titled 'Historical Events - 17 objects' with columns: Time, Type, NE Name, NE Source, NE Vendor, NE Model, and Message. The table lists 17 rows of historical event data.

Time	Type	NE Name	NE Source	NE Vendor	NE Model	Message
1996/01/01 03:21...	Historic TCAs	OM3500-2-SP	OC12-12-1-2	NORTEL	OPTera Metro 35...	OC12-12-1-2:T-C...
1996/01/01 03:23...	Historic Alarms	OM3500-2-SP	OC12-12-1	NORTEL	OPTera Metro 35...	OC12-12-1:MN,...
1996/01/01 03:22...	Historic Alarms	OM3500-2-SP	OC12-12-1	NORTEL	OPTera Metro 35...	OC12-12-1-2:CL,...
1996/01/01 03:21...	Historic Alarms	OM3500-2-SP	OC12-12-1	NORTEL	OPTera Metro 35...	OC12-12-1-2:MJ,...
1996/01/01 03:05...	Historic Alarms	OM3500-2-SP	OC12-12-1	NORTEL	OPTera Metro 35...	OC12-12-1-2:CL,...
1996/01/01 03:03...	Historic Alarms	OM3500-2-SP	OC12-12-1	NORTEL	OPTera Metro 35...	OC12-12-1-2:MJ,...
1996/01/01 02:56...	Historic Alarms	OM3500-2-SP	OC12-12-1	NORTEL	OPTera Metro 35...	OC12-12-1-2:CL,...
1996/01/01 02:53...	Historic Alarms	OM3500-2-SP	OC12-12-1	NORTEL	OPTera Metro 35...	OC12-12-1-2:MJ,...
1996/01/01 02:49...	Historic Alarms	OM3500-2-SP	OC12-12-1	NORTEL	OPTera Metro 35...	OC12-12-1-2:CL,...
1996/01/01 02:49...	Historic Alarms	OM3500-2-SP	OC12-12-1	NORTEL	OPTera Metro 35...	OC12-12-1-2:MJ,...
2010/01/20 17:20...	Historic Alarms	OM3500-2-SP	OM3500-2-SP	NORTEL	OPTera Metro 35...	Loss of contact wi...
2010/01/20 17:16...	Historic Alarms	OM3500-2-SP	OM3500-2-SP	NORTEL	OPTera Metro 35...	Loss of contact wi...

The results are displayed based on the time zone set in NOC.

Optionally, you can do any of the following:

- Hide or show the Search panel by clicking the **Show/Hide Search Panel** button



- Filter table data. See “[Dynamically filter alarm data](#)” on page 73 for an example of how to do this.
- [“Sort table data” on page 21](#)
- [“Add or remove columns in a table” on page 22](#)
- [“Rearrange the columns in a table” on page 23](#)
- [“Save the visible table data to a file” on page 24](#)

8. To view details about an event, do the following:

- a. Click the **Show/Hide Details Panel** button to display the **Details** panel.



9. Click the event to display details about the event in the Details section of the window, for example:

The screenshot shows the 'Manage Historical Events' window. At the top, there is a search bar with fields for Network Element (OM3500-2-SP), Event Type (Any), Start Date (Jan 19, 2010, 04:37 PM), End Date (Jan 20, 2010, 04:46 PM, Now checked), and Maximum Results (5000). Below the search bar is a table titled 'Historical Events - 17 objects' with columns: Time, Type, NE Name, NE Source, NE Vendor, NE Model, and Message. The table lists 17 entries of historical events. At the bottom of the window, there is a 'Details' panel for the first event listed, which includes fields for Time (1996/01/01 03:21:58), Message (OC12-12-1-2:T-CVP, TC,01-01,03-21-58,FEND,RCV,16,15,15-MIN:\\"T-CVP\\), Type (Historic TCAs), and Network Element (Name: OM3500-2-SP, Model: OPTera Metro 3500 MSP, Source: OC12-12-1-2, Vendor: NORTEL).

You can hide the Details section by clicking the **Show/Hide Details Panel** button. To display the Details section again, click the button again.

## 8 Performing maintenance

---

The specific maintenance commands that you can use and the resources on which you can use them depend on the type of NE that you are working with, the resource type that you are working with (NE, circuit pack, port, or interface), and the permissions that you have been assigned.

This section explains how to:

- “Remove resources from service and return them to service” on page 85
- “Reset NEs, circuit packs, and ports (warm or cold)” on page 86
- “Test loopbacks on interfaces or ports” on page 87
- “Manage protection settings” on page 89

This section does not cover the maintenance commands available using the Maintenance option in the menu bar. They are covered in “[Menu bar commands](#)” on [page 12](#).

The main section of the Maintenance menu can contain up to four sub-items, each one with multiple sub-items:

- Reset
- Protection
- State Change
- Test

If you are using Ethernet services, other items will be available. See “[Configuring and using Ethernet OAM](#)” on [page 133](#) for details.

However, if any of the sub-items itself contains only one item, then it is removed. For example, if the Reset menu contains only the Cold Reset item, then the path will be Maintenance → Cold Reset instead of Maintenance → Reset → Cold Reset.

The procedures in this chapter show the full path.



Note: If while using the NOC you do not see menu items, tabs or buttons that are described in this documentation, it is because the Network Integrity administrator has not assigned the permission to your user account, or the feature has not been installed.



Note: This section describes standard maintenance commands. An NE, circuit pack, port, or interface may also support custom maintenance commands. Details about additional commands are provided in the adapter note for the NE. Consult your system administrator for more information.

## 8.1 Remove resources from service and return them to service

Use this procedure to remove the following resource types from service and return them to service:

- circuit packs
- ports
- interfaces

These commands are not available for NEs.

For circuit packs and ports, only the applicable command is displayed. For example, if a port has been removed from service, then only the “Return to Service” option is shown.

However, for interfaces, this information is not available to the NOC, so both items are always shown. For example, the “Return to Service” item is always displayed, even if an interface is already “In Service”. If you choose this option, the NOC simply displays a message that the request is successful.

The following table lists and describes the available state change commands.

**Table 8–1: State change commands**

Command name	Description
Remove from Service	Sends a request to the NE, through the adapter, to take the selected resource out of service.
Return to Service	Sends a request to the NE, through the adapter, to bring the selected resource back into service.



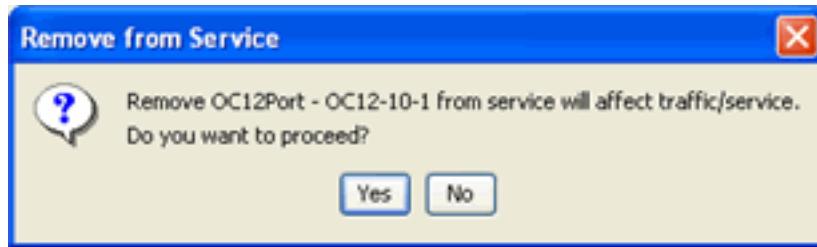
**Note:** You can only send maintenance commands to an NE that is in the Managed state and that is in contact. If the NE is out of contact, the Maintenance menu items are grayed out.



**Note:** Because Network Integrity does not propagate state change notifications from the NE, the state showing in the NOC does not change when you send maintenance commands unless you “[Update inventory in the Network Element View window](#)” on page 52 using the Resync with NE option or perform a data mining operation. Data mining is described in the Network Integrity Framework Configuration Guide.

1. To remove a circuit pack, port, or interface from service:
  - a. In the Network Element View window, right-click the circuit pack, port, or interface and choose **Maintenance** → **State Change** → **Remove From Service**.

- b. Respond to any additional prompts as appropriate. For example, if you remove a port from service, the following confirmation message is displayed:



2. To return a circuit pack, port, or interface to service:
  - a. In the Network Element View window, right-click the circuit pack, port, or interface and choose **Maintenance** → **State Change** → **Return to Service**.

## 8.2 Reset NEs, circuit packs, and ports (warm or cold)

Use this procedure to perform a warm or cold reset on any of the following resource types:

- NEs
- circuit packs
- ports

These commands are not available for interfaces.

The following table lists and describes available reset commands.



**Note:** Resources will have either a Reset command or Warm Reset/Cold Reset commands, not both.

**Table 8–2: Reset commands**

Command name	Description
Reset	Sends a request to the NE, through the adapter, to cause a reset on the selected resource. This command may impact traffic depending on how the command is defined in the adapter.
Warm Reset	Sends a request to the NE, through the adapter, to cause a warm reset on the selected resource. Typically, a warm reset is non-service affecting.
Cold Reset	Sends a request to the NE, through the adapter, to cause a cold reset on the selected resource. Typically, a cold reset is service affecting, although it does not remove the selected resource from service.



**Note:** You can only send maintenance commands to an NE that is in the Managed state and that is in contact. If the NE is out of contact, the Maintenance menu items are grayed out.



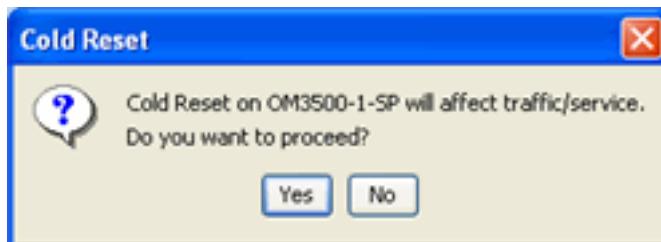
Note: Because Network Integrity does not propagate state change notifications from the NE, the state showing in the NOC does not change when you send maintenance commands unless you “[Update inventory in the Network Element View window](#)” on page 52 using the Resync with NE option or perform a data mining operation. Data mining is described in the Network Integrity Framework Configuration Guide.

1. Do one of the following:

If you want to	Then
reset an NE	in the Network Elements table or the Topology view, right-click the NE and choose one of: <ul style="list-style-type: none"> <li>• Maintenance → Reset → Warm Reset</li> <li>• Maintenance → Reset → Cold Reset</li> <li>• Maintenance → Reset → Reset</li> </ul>
reset a circuit pack or port	In the Network Element View window, right-click the circuit pack or port and choose one of: <ul style="list-style-type: none"> <li>• Maintenance → Reset → Warm Reset</li> <li>• Maintenance → Reset → Cold Reset</li> <li>• Maintenance → Reset → Reset</li> </ul>

2. Respond to any additional prompts as appropriate.

For example, if you perform a cold reset on an NE, the following confirmation message is displayed:



A cold reset does not remove the selected resource from service.

## 8.3 Test loopbacks on interfaces or ports

Use this procedure to test loopbacks on any of the following types of resources:

- interfaces
- ports

These commands are not available for circuit packs or NEs.

The following table lists and describes loopback commands.

**Table 8–3: Loopback commands**

Command name	Description
Enable Local Loopback	Sends a request to the NE, through the adapter, to cause a local loopback to be enabled on the interface. A local loopback will cause egress traffic on the specified interface to be looped back and sent back into the NE on the same interface.
Enable Remote Loopback	Sends a request to the NE, through the adapter, to cause a remote loopback signal to be generated on the selected interface. A remote loopback will cause a request to be sent on the specified interface to the far end asking for the far end to loop its ingress traffic back to the selected interface.
Enable Network Loopback	Sends a request to the NE, through the adapter, to cause a network loopback to be enabled on the specified interface. A network loopback will cause ingress traffic on the selected interface to be looped back and sent back out onto the same interface.



Note: You can only send maintenance commands to an NE that is in the Managed state and that is in contact. If the NE is out of contact, the Maintenance menu items are grayed out.



Note: Because Network Integrity does not propagate state change notifications from the NE, the state showing in the NOC does not change when you send maintenance commands unless you “[Update inventory in the Network Element View window](#)” on page 52 using the Resync with NE option or perform a data mining operation. Data mining is described in the Network Integrity Framework Configuration Guide.

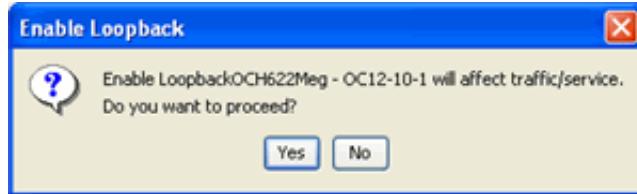
1. To enable a loopback:

- a. In the Network Element View window, right-click the port or interface and choose **Maintenance** → **Test** → <Command>, where <Command> is one of the following:
  - Local Loopback
  - Remote Loopback
  - Network Loopback

See “[Loopback commands](#)” on page 88 for details about local, remote, and network loopbacks.

- b. Respond to any additional prompts as appropriate.

For example, the following prompt is displayed when you enable a local loopback.



## 8.4 Manage protection settings

Use this procedure to manage protection settings on any of the following types of resources:

- circuits packs
- ports
- interfaces

These commands are not available for NEs.

The following table lists and describes protection commands.

**Table 8–4: Protection commands**

Command name	Description
Clear	Clears the Force, Manual, or Lockout command. For Force or Manual commands, traffic does one of the following: <ul style="list-style-type: none"> <li>• non-revertive — traffic remains on the protecting resource until another switch request is issued</li> <li>• revertive — traffic returns to the working resource immediately</li> </ul>
Manual	Switches all traffic to the protecting resource. If there is a failure on the protecting resource while the Manual switch is in place, traffic switches back to the working resource. Once the failure is cleared, traffic switches back to the protecting resource.
Force	Switches all traffic to the protecting resource. If there is a failure on the protecting resource while the Force switch is in place, traffic switches back to the working resource. Once the failure is cleared, traffic switches back to the protecting resource. <p>Note that a Force switch overrides a Manual switch.</p>
Lockout	Prevents traffic from switching to the protecting resource. <p>If the working resource fails while the lockout is applied, traffic will drop.</p> <p>A lockout overrides both a Force switch and a Manual switch.</p>
Exercise	Exercises traffic protection switching on the resource without completing the actual switch.



Note: You can only send maintenance commands to an NE that is in the Managed state and that is in contact. If the NE is out of contact, the Maintenance menu items are grayed out.



Note: Because Network Integrity does not propagate state change notifications from the NE, the state showing in the NOC does not change when you send maintenance commands unless you [“Update inventory in the Network Element View window” on page 52](#) using the Resync with NE option or perform a data mining operation. Data mining is described in the Network Integrity Framework Configuration Guide.

1. To apply a forced switch or manual switch to a resource, in the Network Element View window, right-click the circuit pack, port, or interface and choose **Maintenance** → **Protection** → <Command>, where <Command> is one of the following:
  - Force
  - Manual

See “[Protection commands](#)” on page 89 for details about forced and manual switches.
2. To lock out a resource, in the Network Element View window, right-click the circuit pack, port, or interface and choose **Maintenance** → **Protection** → **Lockout**.
3. To clear a forced switch, manual switch, or lock out, right-click the circuit pack, port, or interface and choose **Maintenance** → **Protection** → **Clear**.
4. To exercise protection switching, right-click the circuit pack, port, or interface and choose **Maintenance** → **Protection** → **Exercise**.
5. Respond to any additional prompts as appropriate.

# 9 Monitoring performance

When enabled, the Performance Monitoring (PM) Viewer plugin provides a snapshot of the most current PM counts and the last completed bin counts for the interfaces on a network element (NE). PM data counts are retrieved directly from an NE and presented in the PM Viewer.

The PM Viewer is launched as a stand-alone window from a circuit pack, port, or interface in the Network Element View window. Any number of PM Viewer windows can be opened at a time.

This section contains the following information and procedures for using the PM Viewer:

- “About the PM Viewer” on page 91
- “Display PM counts” on page 93
- “Change the appearance of the graphical view” on page 97
- “Zoom in and out of the graphical view” on page 101
- “Export graphical or tabular data to a file” on page 102
- “Refresh performance monitoring data” on page 102



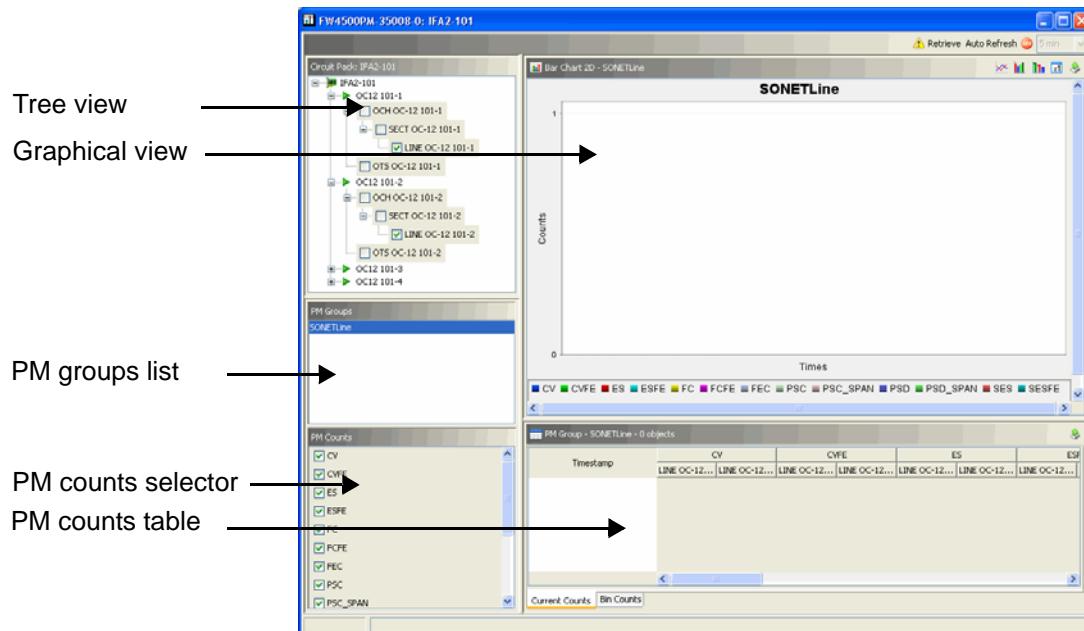
**Note:** If while using the NOC you do not see menu items, tabs or buttons that are described in this documentation, it is because the Network Integrity administrator has not assigned the permission to your user account, or the feature has not been installed.

## 9.1 About the PM Viewer

The PM Viewer is accessed from the Network Element View window. The counts that can be viewed depend on the PM groups supported by the adapter. The PM Viewer consists of four sections as shown in “[PM Viewer sections](#)” on page 92:

- tree view — The items displayed in the tree view depend on what you selected in the Network Element View window. The tree view shows the item that you selected and any sub-items (for example, if you selected a port in the Network Element View window, the tree view shows the port, which can be expanded to view the interfaces associated with the port). You can expand the items to select the interfaces in the tree view for which to view PM counts.
- graphical view — The graphical view displays the PM counts in a line graph or bar chart. You can export the graph or chart to a PNG file.
- PM groups list — The PM groups list shows the PM groups that are available for the interface that you selected in the tree view. If you select more than one interface in the tree view, only the groups that they have in common are shown in the PM groups list. If the interfaces are at different layers (for example, if you select a line interface and a section interface), the PM groups list is empty. You can select only one PM group at a time in the PM groups list.

- PM counts selector — The PM counts selector shows the PM counts available within the group. You can select any or all PM counts to be displayed in the graphical view.
- PM counts table — The PM counts table shows the PM counts in the group in tabular format for as many interfaces as you have selected in the tree view. You can export this information to a CSV or TSV file.

**Figure 9–1: PM Viewer sections**

### 9.1.1 About current counts and bin counts

NEs keep the PM data in "bins" that cover a period of time, for example, 15 minutes or 1 hour. In the PM counts table, you can choose the Current Counts tab or the Bin Counts tab.

Current counts show the most recent data available for a PM Group. This data is for the current partial bin (or partially complete time period).

Completed bins are shown in the bin counts view.

### 9.1.2 About polling periods and intervals

For current counts, the maximum period for polling is 100 polling cycles. For example, if you set the interval to poll every 5 minutes, then polling would occur for a period of 500 minutes (100 cycles x 5 minutes). The available intervals are:

- 10 seconds
- 20 seconds
- 30 seconds
- 1 minute
- 3 minutes

- 5 minutes

## 9.2 Display PM counts

Use this procedure to display PM counts in the PM Viewer. You can access the PM Viewer at several different levels in the Network Element View (circuit pack, port, or interface) by right-clicking the item and choosing Performance > PM Viewer.

This level determines how many interfaces you can access in the PM Viewer:

- circuit pack — provides access to all interfaces on the pack
- port — provides access to all interfaces on the port
- interface — provides access only to the selected interface

See “[About the Resource Tree](#)” on page 46 for more information about how circuit packs, ports, and interfaces are represented in the Network Element View.

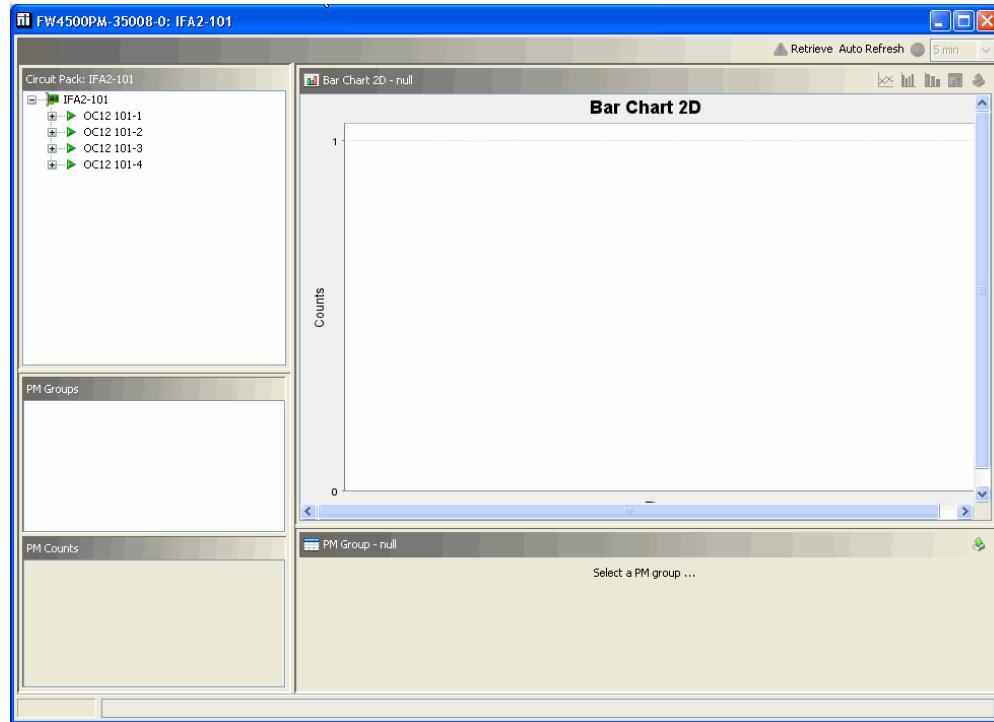


**Note:** The network adapter controls the counts that are available for an NE. If you do not see a PM group or count in the PM Viewer, it is not supported by the deployed adapter.

1. [“View shelf, circuit pack, port, and interface details” on page 48](#).
2. Choose the level at which you want to view PM counts.

If you want to	Go to step
view PM counts at the circuit pack level  This will enable you to use the PM Viewer tree view to navigate through the ports on a circuit pack and choose one or more interfaces for which to view PM counts.	3.
view PM counts at the port level  This will enable you to use the PM Viewer tree view to choose one or more interfaces on a port for which to view PM counts.	4.
view PM counts at the interface level  This option enables you to view PM counts for the interface that you chose.	5.
3. Right-click the circuit pack for which you want to view current PM counts and select <b>Performance &gt; PM Viewer</b> .  The system displays the PM Viewer with the circuit pack as the top level in the tree view, as shown in the following figure.	

By default, no interfaces are selected, and the PM groups list, PM counts table, and graphical view are empty. Go to [Step 6](#).



4. Drill down to select the port for which you want to view current PM counts, right-click the port and select **Performance > PM Viewer**.

The system displays the PM Viewer with the port as the top level in the tree view.

By default, no interfaces are selected, and the PM groups list, PM counts table, and graphical view are empty, as shown in the example in step 3. Go to [Step 6](#).

5. Drill down to select the interface for which you want to view current PM counts, right-click the interface and select **Performance > PM Viewer**.

The system displays the PM Viewer with:

- the interface selected in the tree view
- the first group in the PM groups list selected
- a 2-dimensional bar chart that shows the PM counts displayed in the graphical view. By default, the first four counts in the group are selected.

#### To select the interfaces for which to view PM counts

6. If you accessed the PM Viewer from a circuit pack or port, select one or more interfaces for which to view PM counts by expanding the port or the circuit pack and ports in the tree view.

By default:

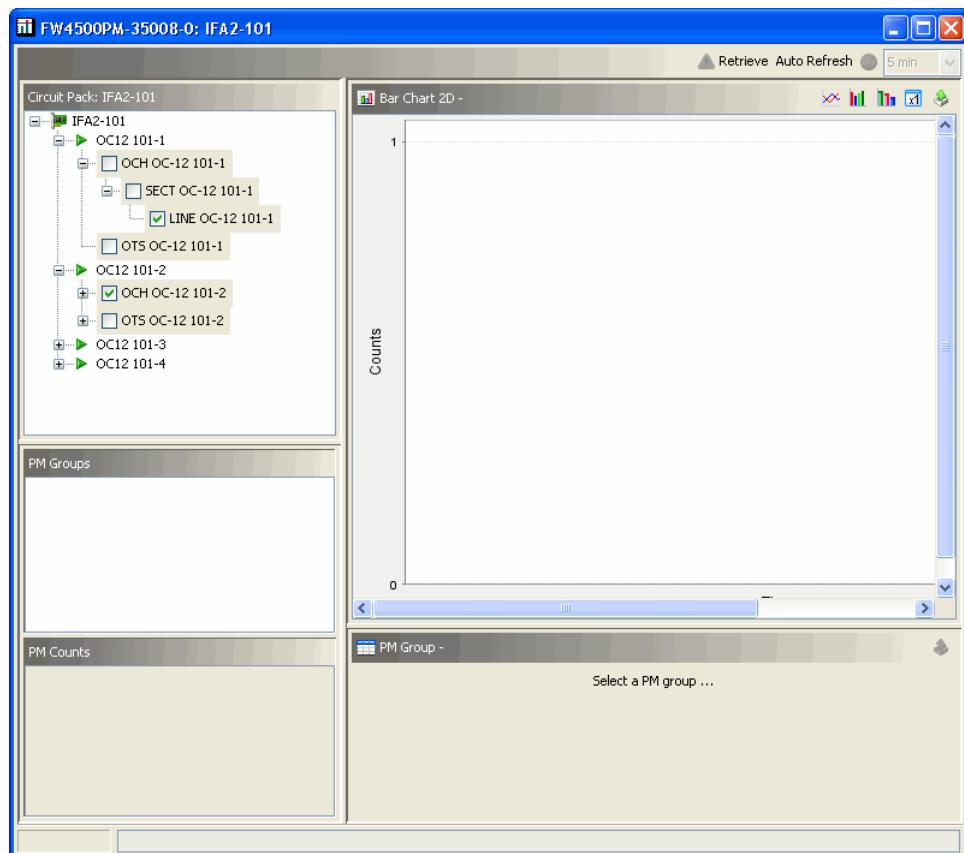
- The first group in the PM groups list is selected.
- The PM counts table is updated to show the current counts for the selected group, sorted by timestamp.

- The graphical view is updated to show a 2-dimensional bar chart for the selected group. By default, the first four counts in the group are selected.
- the Current Counts tab is selected

If you selected multiple interfaces, in the PM counts table, the interface label is used as a sub-column heading within the PM count column, as shown in the following example.

CV	ES			
DS3T3AndDS3-6-1	DS3T3AndDS3-6-2	DS3T3AndDS3-6-1	DS3T3AndDS3-6-2	DS3T3AndDS3-6-1
2	3	4	5	6

Note that the interfaces that you choose must all be at the same level, which means that they may have PM counts in common. If the interfaces that you select are at different levels (section and line, for example), no groups or PM counts will be available to choose, as shown in the following example.



7. To clear the interface from the PM counts table and graphical view, deselect the check box in the tree view.

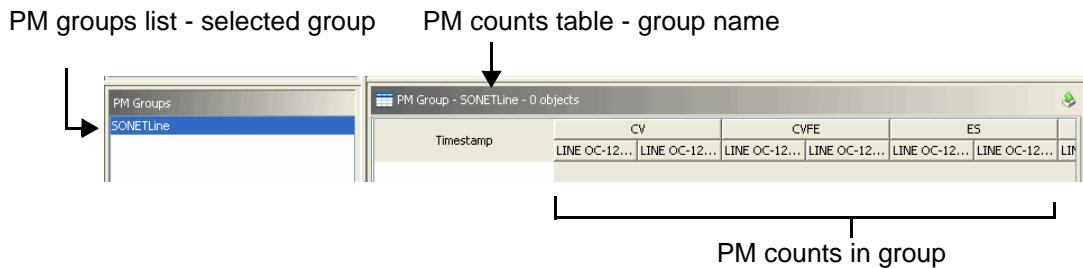
If you deselect all check boxes in the tree view, the PM groups list, PM counts table, and graphical view will all be empty.

#### To change the PM counts that are displayed

8. Select a different group in the PM groups list.

You can select only one group at a time.

The PM counts table is updated to show the PM counts in the group for each interface that you chose.



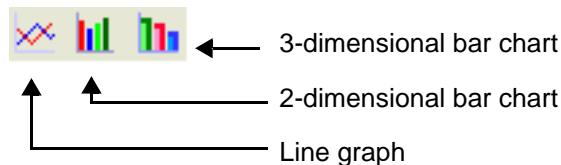
### To view bin counts

- In the PM counts table, click the Bin Counts tab.

For more information about current counts and bin counts, see [“About current counts and bin counts” on page 92](#).

### To change the PM counts displayed in the graphical view

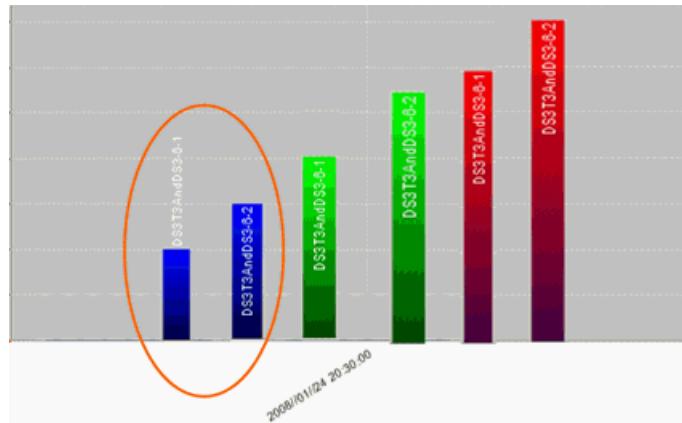
- In the graphical view, do the following:
  - In the PM counts list, select the check boxes for the PM counts that you want to view.
  - Click one of the following icons to display the data as a line graph, 2-dimensional bar chart, or 3-dimensional bar chart:



The system displays the corresponding line graph, 2-dimensional bar chart, or 3-dimensional bar chart and a legend is displayed that shows the count names.

If you select a different interface, group, or count, the chart or graph is updated to show the new values.

If you chose multiple interfaces, the interface name is displayed in the bar chart in the bar, as shown in the following example. In the circled area, there is not enough room for the label within the bar, so it is displayed above.



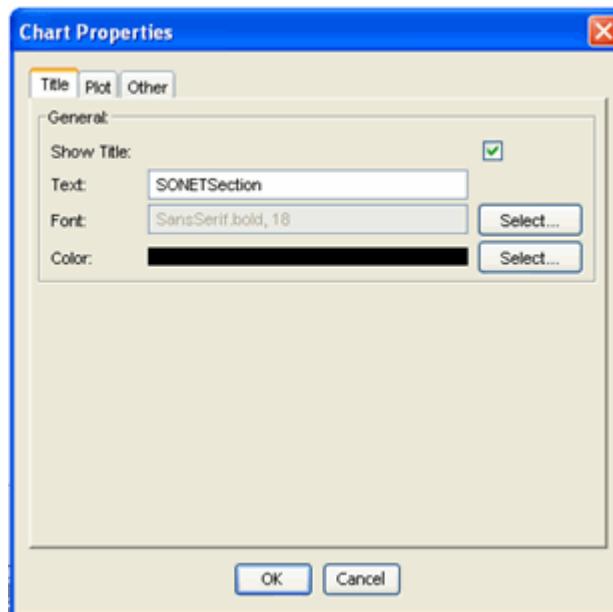
Note: Multiple interfaces are only shown for current counts, not bin counts.

## 9.3 Change the appearance of the graphical view

Use this procedure to change the appearance of the title, axes, or background. Changes that you make are not saved when you close the PM Viewer window.

1. Right-click the chart or graph, choose **Properties**.

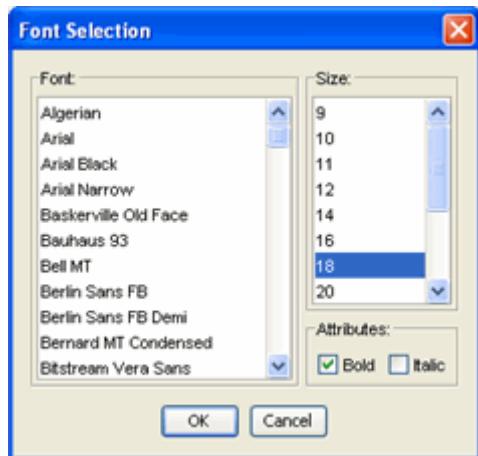
The **Chart Properties** dialog box opens with the Title tab selected by default.



### To change the appearance of the title

2. If you do not want to show the title, clear the **Show Title** check box.
3. To change the text of the title, type the new title in the **Text** box.

4. To change the font of the title, click the **Select** button next to the **Font** box.  
The system displays the **Font Selection** dialog box.

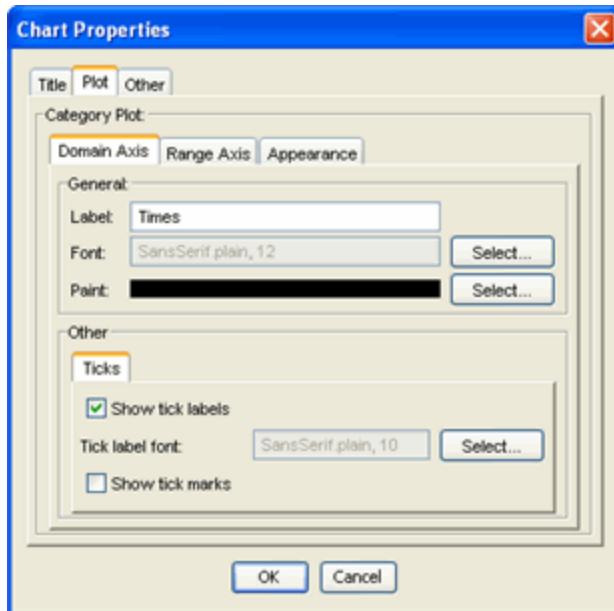


5. Choose a font and size, and if required, enable the **Bold** check box to display the title in bold and the **Italic** check box to display the title in italics. Click **OK**.
6. To change the color of the text, click the **Select** button next to the **Color** box, choose a new color, and click **OK**.

#### To change the appearance of the axes or chart

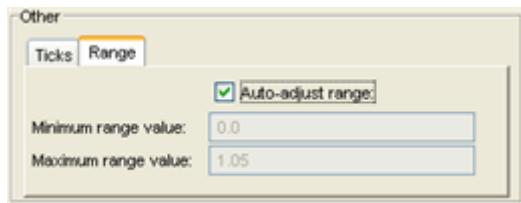
7. In the **Chart Properties** dialog box, click the **Plot** tab.

The **Plot** tab opens with the **Domain Axis** tab selected by default.



8. To change the labels on the axis, do the following:
  - a. To change the text of the label, type the new label in the **Label** box.

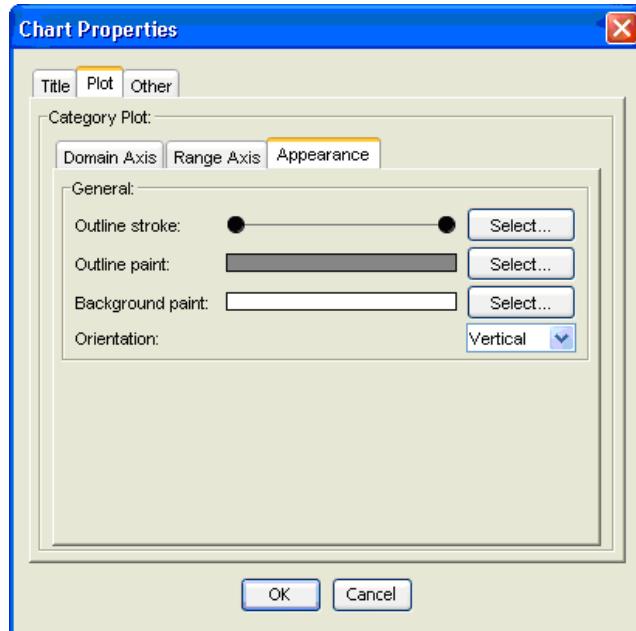
- b. To change the font of the title, click the **Select** button next to the **Font** box, choose a font and size, and if required, enable the **Bold** check box to display the title in bold and the **Italic** check box to display the title in italics. Click **OK**.
  - c. To change the color of the text, click the **Select** button next to the **Paint** box, choose a new color, and click **OK**.
9. To change the appearance of the tick marks on the axis, do the following:
  - a. To remove the labels on the tick marks, clear the **Show Tick Labels** check box.
  - b. To change the font of the tick labels, click the **Select** button next to the **Tick Label Font** box, choose a font and size, and if required, enable the **Bold** check box to display the labels in bold and the **Italic** check box to display the labels in italics. Click **OK**.
  - c. To show tick marks, select the **Show Tick Marks** check box.
10. To change the labels or tick marks on the range axis, click the **Range Axis** tab and do [Step 8.](#) and [Step 9.](#)
11. To modify the range options on the **Range Axis** tab, click the **Range** tab in the **Other** section.



12. Clear the **Auto-Adjust Range** check box and type values in the **Minimum Range Value** and **Maximum Range Value** check boxes to define the new range.

### To change the appearance of a line graph

13. Click the **Appearance** tab.

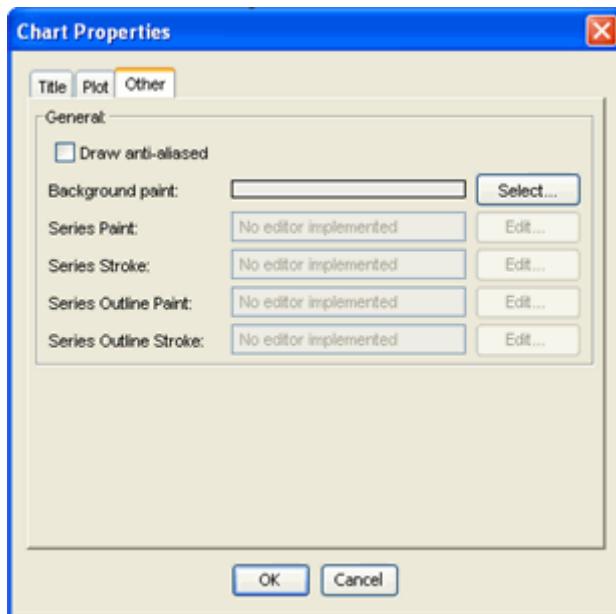


14. Do any of the following:
  - a. To change the line stroke, click the **Select** button next to the **Outline Stroke** example, choose a new stroke, and click **OK**.
  - b. To change the line color, click the **Select** button next to the **Outline Paint** example, choose a new color, and click **OK**.
  - c. To change the background color, click the **Select** button next to the **Background Paint** example, choose a new color, and click **OK**.
  - d. To change the orientation, select a new orientation for the **Orientation** list.

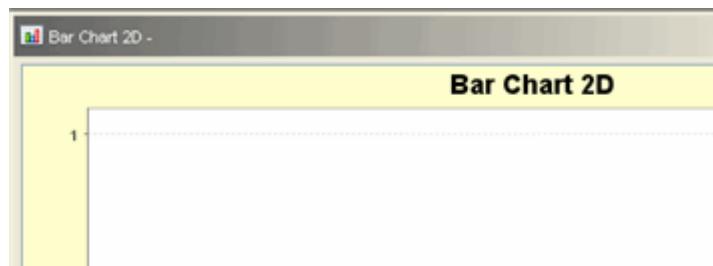
### To change anti-alias properties or background color

15. In the **Chart Properties** dialog box, click the **Other** tab.

The **Other** tab opens.



16. If you do not want the image to be anti-aliased, clear the **Draw Anti-Aliased** check box.  
By default, the drawn lines and bars are anti-aliased.
17. To change the background color, click the **Select** button next to the **Background Paint** box choose a new color, and click **OK**.  
In the following example, the background has been changed to light yellow.



#### To apply your changes

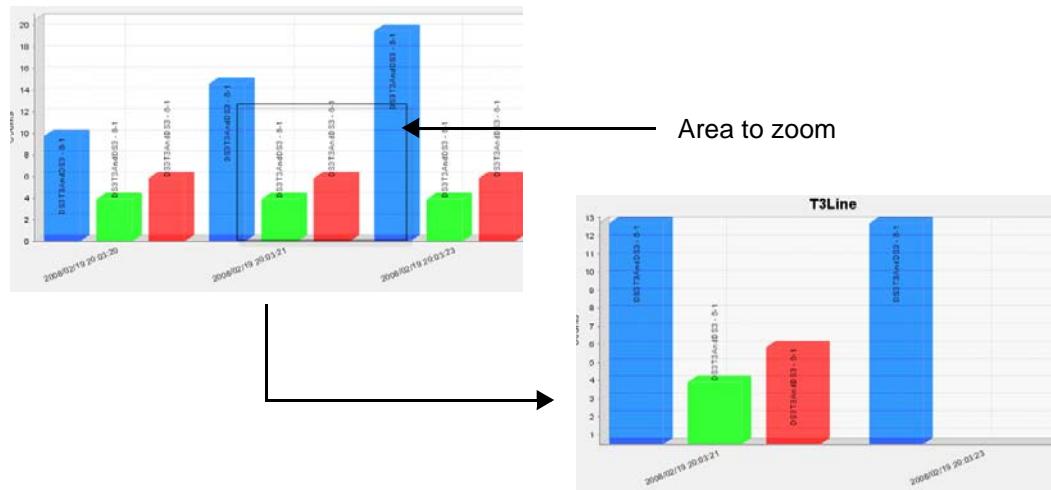
18. In the **Chart Properties** dialog box, click **OK**.

## 9.4 Zoom in and out of the graphical view

Use this procedure to zoom in and out of the graph or chart.

### To zoom in

1. Left-click in the graphical view and drag to draw a box from top left to bottom right around the area that you want to zoom in on.



### To zoom out

2. Right-click in the graphical view and choose **Restore** or draw the selection box in reverse (bottom right to top left).
- The graphical view is reset to its original size.

## 9.5 Export graphical or tabular data to a file

Use this procedure to export the graph or chart shown in the graphical view to a PNG file or to export the data in the PM counts table to a CSV or TSV file.

1. To export the graph or chart to a PNG file:
  - a. Right-click the graph or chart and choose **Save As** or click the **Export** icon at the top right of the graphic.



The **Save As** window opens.

- b. Navigate to the folder where you want to export the file, type a file name, and click **Save**.
2. To export the data in the PM counts table to a file, see “[Save the visible table data to a file](#)” on page 24.

When PM data is exported from the PM Viewer, the system saves the data for the currently selected tab combinations, such as “Current Counts - SONET Line”, or “Bin Counts - SONET Physical”.

## 9.6 Refresh performance monitoring data

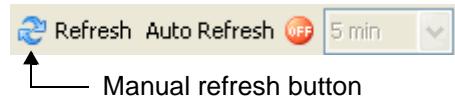
Use this procedure to refresh the performance monitoring data displayed in the PM Viewer. You can refresh the data manually or automatically at specified intervals.

- Manual refresh — Manual refresh is available for current counts or for bin counts. If you click the Refresh button, existing data is discarded, the counts are retrieved again, and the new values are displayed. Note that the first time data is retrieved, this button is labeled Retrieve.
- Auto refresh — Auto refresh is available only for current counts. When auto-refresh is selected, the PM Viewer will begin to poll the current counts from the NE every polling interval for up to 100 polling cycles (see “[About polling periods and intervals](#)” on page 92). The data from each poll will constitute a row in the PM Viewer. At the end of the 100 polls the auto-refresh will be disabled but the data will remain in the table. You can manually disable auto-refresh by clicking the Auto Refresh button at any time and the collected data will remain in the table.

1. [“Display PM counts” on page 93.](#)

**To manually refresh the data**

2. Click the Refresh button.

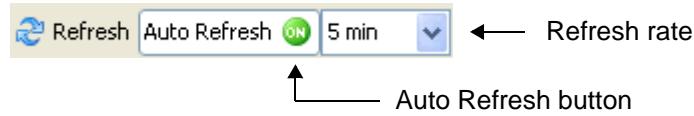


Existing data is discarded, the counts are retrieved again, and the new values are displayed.

**To automatically refresh the data (current counts only)**

3. Click the Auto Refresh button.

The status indicator changes from Off to On and the polling interval selection list becomes active.



4. From the list of polling intervals, select the refresh rate: **10 sec, 20 sec, 30 sec, 1 min, 3 min, or 5 min** intervals.

The data will remain in the table until another refresh is performed.

**To disable auto-refresh**

5. Click the Auto-Refresh button again.

The status indicator changes from On to Off and the polling interval selection list is grayed out. The last set of data will remain in the table.

# 10 Managing interfaces

---

Network Integrity detects far-end interfaces if they are supported by the NE and the installed NE adapter. In the shelf level graphics window, you can set and delete far-end interfaces from ports.



**Note:** The procedures in this section affect only the display of the interfaces in the NOC GUI. They do not impact the configuration of NEs in the network. When the far end interface is set using the NOC, it does not set any parameters on the NE. Everything is local to the NOC. The interface details show attributes against an interface that have been populated during data mining for an NE's logical inventory. When the far end interface field is cleared, nothing is set or changed on the NE. The transmitted section trace information can only be set using the TL1 Command and Control plugin in the NOC.

This section contains the following procedures for managing interfaces:

- “[Define a far-end interface for a near-end interface](#)” on page 104
- “[Clear a far-end interface setting](#)” on page 106



**Note:** If while using the NOC you do not see menu items, tabs or buttons that are described in this documentation, it is because the Network Integrity administrator has not assigned the permission to your user account, or the feature has not been installed.

## 10.1 Define a far-end interface for a near-end interface

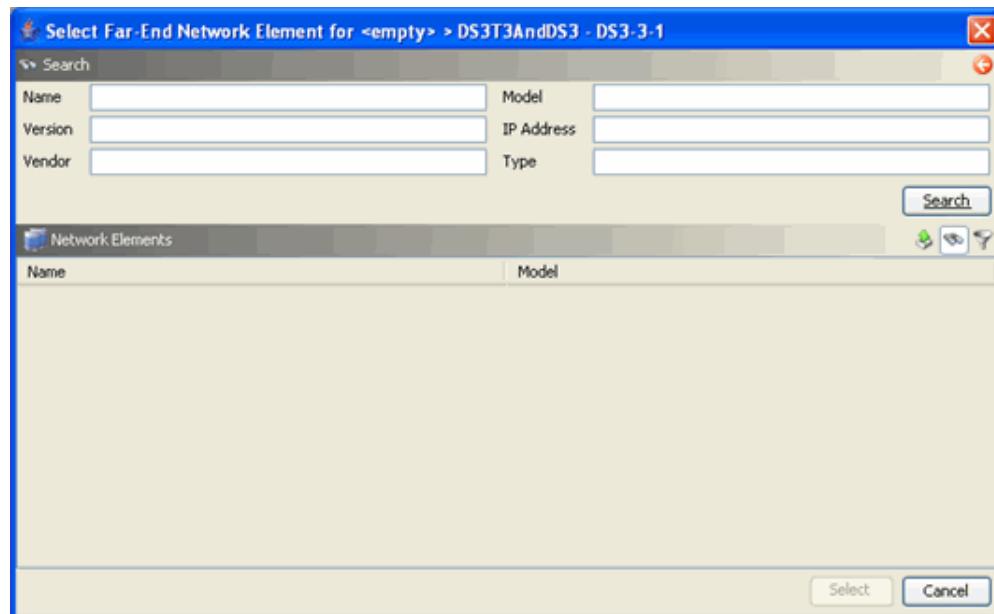
Use this procedure to override the far-end interface setting that has been set by Network Integrity. After you perform this procedure, the value persists in the NOC, even if the network configuration is different. If, in the future, you want Network Integrity to discover the setting from the network, “[Clear a far-end interface setting](#)” on page 106.



**Note:** The procedure in this section affects only the display of the interfaces in the NOC GUI. It does not impact the configuration of NEs in the network.

1. For the NE on which you want to define a far-end interface, “[View shelf, circuit pack, port, and interface details](#)” on page 48.
2. Right-click the interface for which you want to define a far-end interface and choose **Provisioning > Set Far-End Interface**.

The **Select Far-End Network Element** window opens.

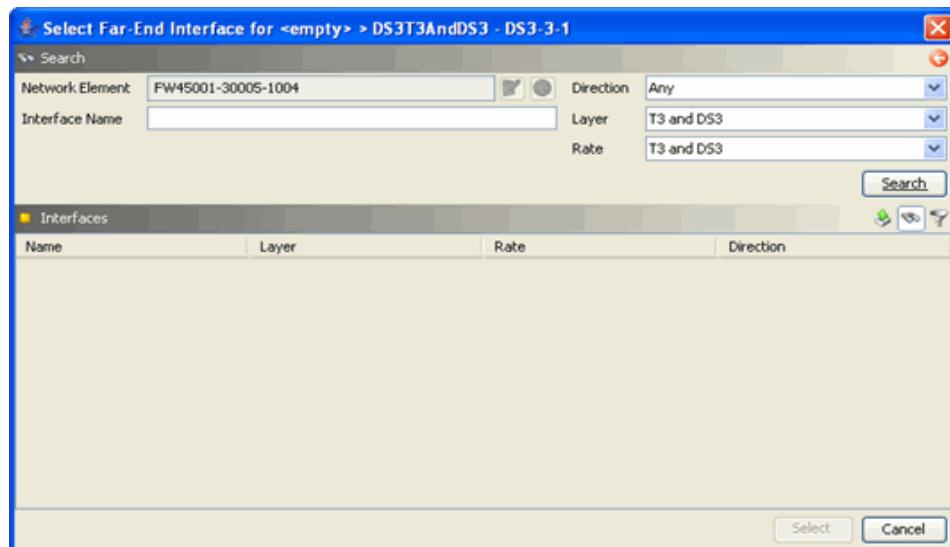


3. Enter the search criteria and click **Search**.

To display a list of all NEs in the network, leave the search criteria blank and click Search.

4. From the list of NEs, choose the far-end NE for the interface and click **Select**.

The Select Far-End Network Element window closes. The **Select Far-End Interface** window opens and the **Network Element** field contains the NE that you selected. The **Direction**, **Layer**, and **Rate** fields contain the values as defined for the near-end interface.



5. Under Search, you can type a value in the **Interface Name** field to identify the interface or leave it blank to search for all interfaces that the NE can connect to. The **Direction**, **Layer**, and **Rate** fields can not be modified.

6. Click **Search**.

The interfaces that match the search criteria are displayed.

7. From the list of interfaces, choose an interface and click **Select**.

The Select Far-End Interface window closes. An information window opens and states that the interface was modified. You can view the far-end interface information by right-clicking the interface in the Network Element View (shelf level graphics) window and choosing Inventory > Details:

- The Far-End Interface field shows the interface that you selected.
- The Far-End Source and Far-End Source Details fields indicate that the interface was modified by a user.
- The Far-End Update Time field shows the time of the update.



Note: If a far-end interface is detected by Network Integrity (not manually specified by a user), the Far-End Source and Far-End Source Details fields indicate that the interface was defined by the network.

## 10.2 Clear a far-end interface setting

Use this procedure to remove a far-end interface from a port. Performing this procedure allows the far-end interface setting in the NOC to be updated from the network, the next time a data mining job is performed by Network Integrity. For information about data mining, see the Network Integrity Framework Configuration Guide.



Note: The procedure in this section affects only the display of the interfaces in the NOC GUI. It does not impact the configuration of NEs in the network.

1. For the NE from which you want to delete a far-end interface, “[View shelf, circuit pack, port, and interface details](#)” on page 48.
2. Right-click the interface from which you want to delete a far-end interface and choose **Provisioning > Delete Far-End Interface**.

An information window opens and states that the interface was deleted.

3. Click **OK**.

You can view the far-end interface information by right-clicking the interface in the Network Element View (shelf level graphics) window and choosing Inventory > Details:

- The Far-End Interface field is empty.
- The Far-End Source and Far-End Source Details fields indicate that the interface was modified by a user.
- The Far-End Update Time field shows the time of the update.

# 11 Managing Ethernet services

The section contains the following procedures performed from the Manage Ethernet Services window:

- “Common Ethernet Services procedures” on page 107
- “Create a Dedicated Internet Access (DIA) service” on page 111
- “Create an E-Line service” on page 116
- “Create an E-LAN service” on page 119
- “Create an E-Tree service” on page 124
- “Activate a pre-provisioned CPE” on page 128
- “Modify an ethernet service” on page 131



**Note:** If while using the NOC you do not see menu items, tabs or buttons that are described in this documentation, it is because the Network Integrity administrator has not assigned the required roles and permissions to your user account, or the feature has not been installed.

## Prerequisite

The user provisioning the ethernet service requires a work order/circuit detail record that contains all parameters including all NEs and interfaces that are part of the service. The Provider Edge (PE) devices must be under management by Network Integrity and must be data mined prior to provisioning the service. CPE devices can be pre-provisioned prior to being installed and turned up. Pre-provisioned CPE devices will not be shown in any NOC views until they are discovered, brought under management and mined for data.

## 11.1 Common Ethernet Services procedures

This section contains procedures that are common to the Manage Ethernet Services dialogs:

- “Display the Manage Ethernet Services window” on page 107
- “Search for an NE or interface and select it” on page 109

### 11.1.1 Display the Manage Ethernet Services window

Use this procedure to display the Manage Ethernet Services window which is available from a variety of locations in the NOC:

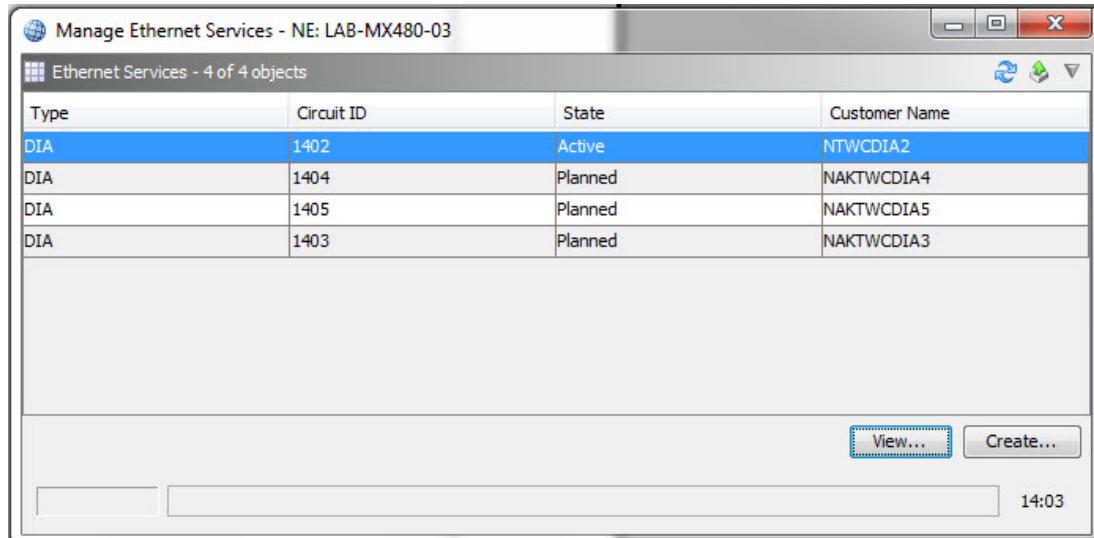
- from an NE in the Network Elements table
- from an NE in the topology view
- from an NE or interface in the shelf level graphics view

From the Manage Ethernet Services window you can View an existing service or Create a new one.

1. Select the desired network element in either the Network Elements table, the topology view, or the NE or interface in the shelf level graphics.

2. Right-click the NE or interface and select **Provisioning > Manage Ethernet Services**.

The Manage Ethernet Services window opens and displays the list of existing services, as in this example.



The main Manage Ethernet Services window displays the following information for each service:

- **Type**: the type of service: DIA, E-Line, E-LAN, or E-Tree
- **Circuit ID**: the identifier for the ethernet service
- **State**: the overall state of the ethernet service: Active, Planned or Partial.
- **Customer Name**: the name of the customer associated with the ethernet service

3. To display the details of a service, select the desired service and click the **View...** button, or right-click and select **View**.

For the procedure, see “[View the details of an ethernet service](#)” on page 110.

4. To create a new ethernet service, click the **Create...** button and select the desired service.

To complete the creation see the following procedures:

- “[Create a Dedicated Internet Access \(DIA\) service](#)” on page 111
- “[Create an E-Line service](#)” on page 116
- “[Create an E-LAN service](#)” on page 119
- “[Create an E-Tree service](#)” on page 124

5. To activate a service, see “[Activate a pre-provisioned CPE](#)” on page 128.

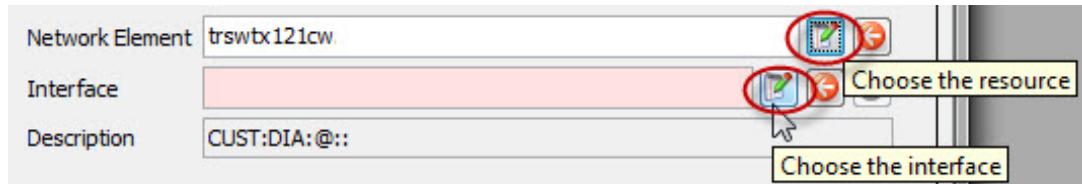
6. To modify a service, see “[Modify an ethernet service](#)” on page 131.

## 11.1.2 Search for an NE or interface and select it

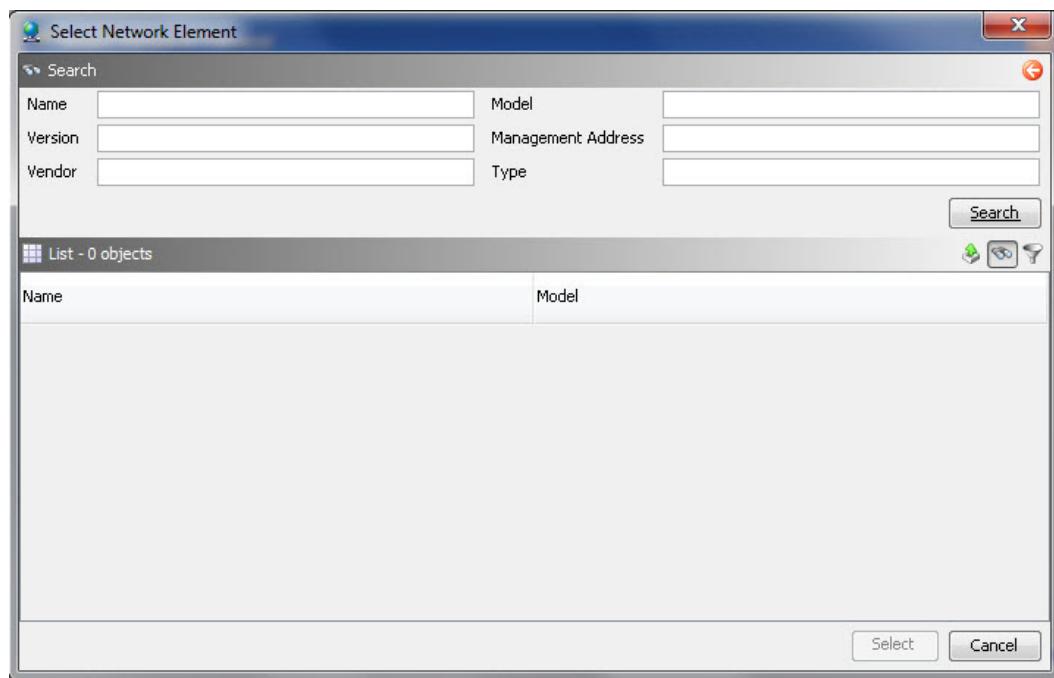
Use this procedure when creating an ethernet service to search for an NE or interface and select it.

The “Choose interface” selector only becomes active when an NE is selected. The Interface search displays interfaces on the selected NE.

- Click the **Choose** button next to the **Network Element** or the **Interface** field.



The Select Network Element or Select Interface window opens, as shown in this NE example.



- Type or select the search criteria in the fields provided and click **Search**.

To search for all NEs or interfaces, leave the search fields blank and click Search. Note that a maximum of 500 results will be displayed.

**Note:** When the Search button is underlined, it indicates that no search has been performed using the currently defined criteria. If the results table is empty and Search is not underlined, this indicates that the search has returned no results.

In the search results list, you can do any of the following:

- Hide or show the Search panel by clicking the **Show/Hide Search Panel** button

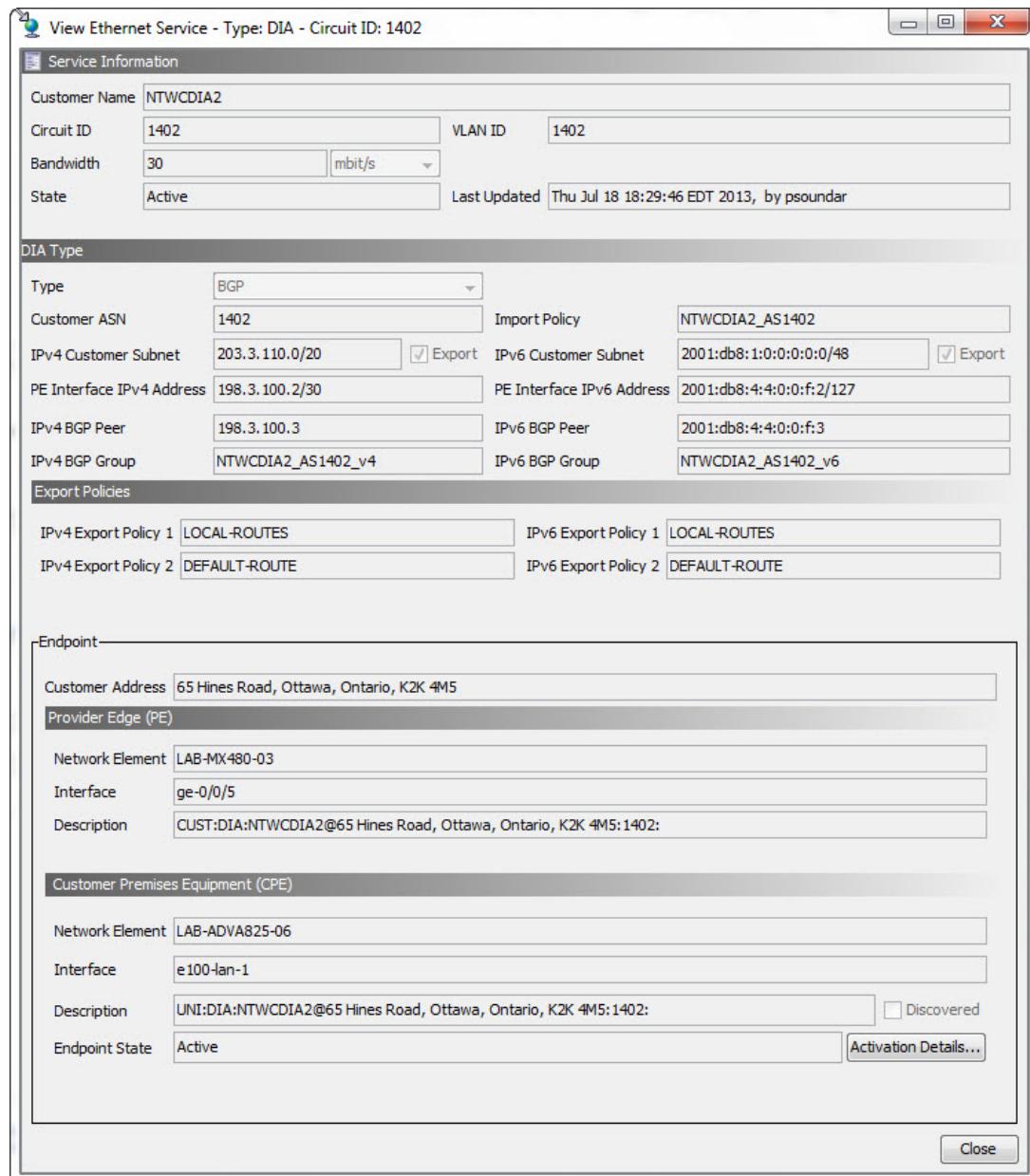
- Filter table data. See “[Dynamically filter alarm data](#)” on page 73 for an example of how to do this.
  - “[Sort table data](#)” on page 21
  - “[Rearrange the columns in a table](#)” on page 23
  - “[Save the visible table data to a file](#)” on page 24
3. Choose an NE or interface in the list and click **Select**.  
The NOC places the selected item in the Network Element or Interface field.

## 11.2 View the details of an ethernet service

Use this procedure to view the details of an existing ethernet service.

1. “[Display the Manage Ethernet Services window](#)” on page 107.
2. From the list of existing services, select the desired service and click **View**.

The view window opens for the selected service, as in this DIA BGP example.



For an explanation of fields for each type of Ethernet service, see the following tables:

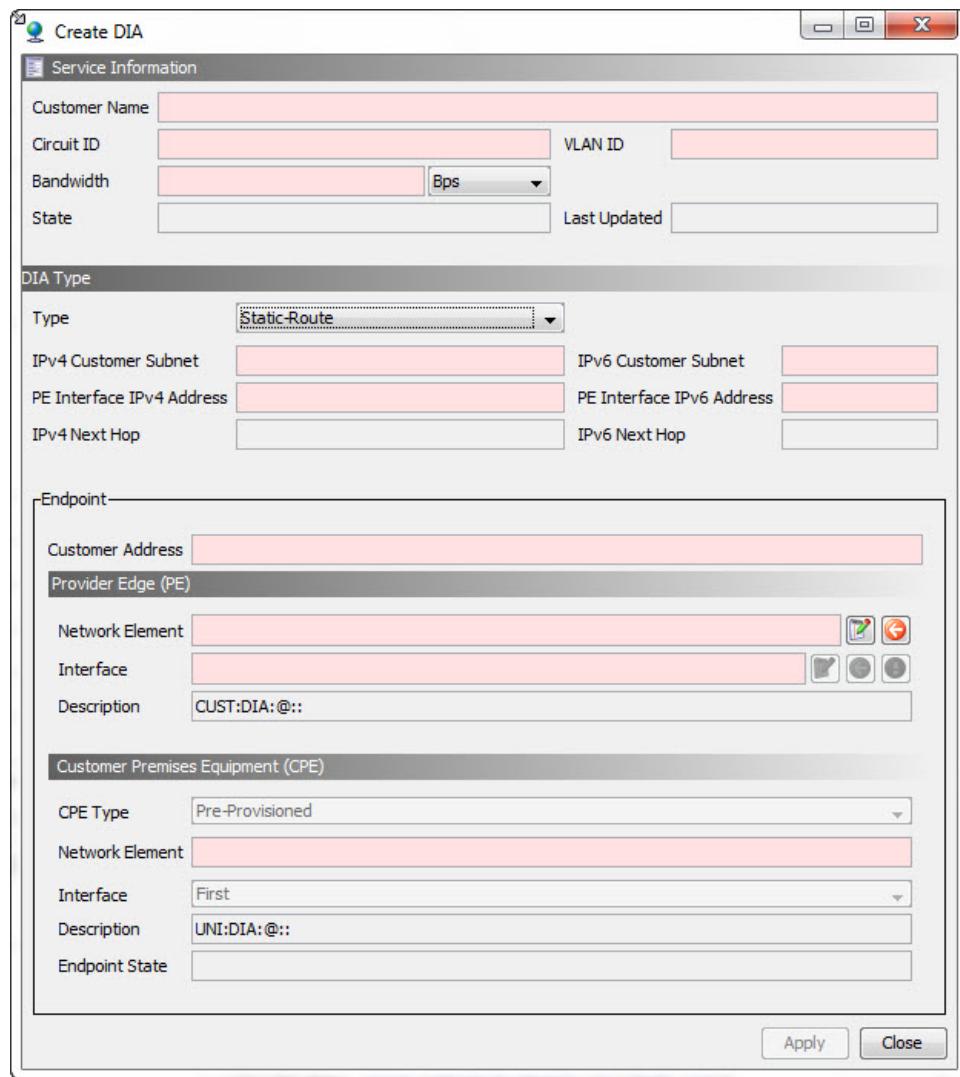
- “[DIA values](#)” on page 112
- “[E-Line values](#)” on page 117
- “[E-LAN values](#)” on page 121
- “[E-Tree values](#)” on page 125

## 11.3 Create a Dedicated Internet Access (DIA) service

Use this procedure to create a Dedicated Internet Access (DIA) service.

The following figure shows the create Dedicated Internet Access dialog box.

**Figure 11–1: Dedicated Internet Access dialog box**



The following table explains the values in the dialog box.

**Table 11–1: DIA values**

Field	Description
<b>Service Information</b>	
Customer Name	The name of the customer for the service.
Circuit ID	The identifier for this network connection.
VLAN ID	The numeric identifier for the VLAN used by the service.
Bandwidth	The bandwidth measurement for the service: Bps, Kbps, Mbps, Gbps, or Tbps.

Field	Description
State	<p>The overall state of the service:</p> <ul style="list-style-type: none"> <li>• ACTIVE: all devices associated with the service are configured in the network.</li> <li>• PARTIAL: one or more devices that make up the service have been configured, but there are additional devices that need to be configured to complete the service.</li> <li>• PLANNED: all CPEs in the service are pre-provisioned in the Network Integrity database but the configuration has not been sent to the network.</li> </ul>
Last Updated	The date and time that the service was last updated
<b>DIA Type</b>	
Type	<p>The type of service: Directly Connected (LAN), Static Route or BGP.</p> <p><b>Note:</b> The fields that appear in the DIA Type area vary according to DIA service type that is selected.</p>
Customer ASN	The Autonomous System Number (ASN) assigned to a customer.
Import Policy	The import policy that contains the route policies.
IPv4 Customer Subnet	IPv4 address of the customer subnet
PE Interface IPv4 Address	IPv4 address of the PE interface
IPv4 Next Hop	Automatically calculated next hop IPv4 address routing
IPv6 Customer Subnet	IPv6 address of the customer subnet
PE Interface IPv6 Address	IPv6 address of the PE interface
IPv6 Next Hop	Automatically calculated next hop IPv6 address routing
IPV4 BGP Peer	IPV4 address of the BGP peer
IPV4 BGP Group	Name of the IPV4 peer group
IPV6 BGP Peer	IPV6 address of the BGP peer
IPV6 BGP Group	Name of the IPV6 peer group
<b>Export Policies</b>	
For Border Gateway Protocol (BGP) type service.	
Export Policies	<p>The policy that is used to advertise or export routes to a customer in the protocol packets:</p> <ul style="list-style-type: none"> <li>• Default</li> <li>• Full</li> <li>• Partial</li> <li>• Partial Default</li> <li>• Full Default</li> </ul>
IPv4 Export Policy 1	First policy to apply to IPv4 routes being exported from the routing table into BGP

Field	Description
IPv4 Export Policy 2	Second policy to apply to IPv4 routes being exported from the routing table into BGP
IPv6 Export Policy 1	First policy to apply to IPv6 routes being exported from the routing table into BGP
IPv6 Export Policy 2	Second policy to apply to IPv6 routes being exported from the routing table into BGP
Authentication Key	BGP authentication key, which is common to the IPv4 and IPv6 stacks. Up to 1024 characters long.
<b>Endpoint</b>	
Customer Address	The address of the customer site for the DIA service.
<b>Provider Edge (PE)</b>	
These values define the PE end of the service.	
Network Element	The NE associated with the service. To select an NE, click the “Choose the resource” button to the right of the field and search for the NE.
Interface	The name of the interface associated with the service. To select an interface, click the “Choose the interface” button to the right of the field and search for the interface on the NE.
Description	The description of the service based on the type of service, the customer address, name, and circuit ID. You cannot directly modify the description. It is updated automatically as you enter the customer name, address, and circuit ID.
<b>Customer Premises Equipment (CPE)</b>	
These values describe the CPE end of the service.	
CPE Type	<p>The type of CPE:</p> <ul style="list-style-type: none"> <li>• Pre-Provisioned: the CPE is being provisioned in advance of being brought under management and being data mined.</li> <li>• Existing: the CPE is under management and has been data mined.</li> <li>• None: no CPE associated with the service. All fields and buttons are disabled.</li> </ul>
Network Element	The CPE network element that connects to the PE equipment.
Interface	<p>The name of the interface on the CPE used to connect to the PE equipment.</p> <p>For pre-provisioned NEs, the interface names are generic. When the NE is brought under management, the name will be updated to what they are on the NE.</p>
Description	<p>The automatically generated description of the service being provided. This field is generated automatically. You cannot directly modify the description.</p>

Field	Description
Endpoint State	The state of the CPE endpoint: <ul style="list-style-type: none"> <li>• ACTIVE: the CPE is under management and the interface is active</li> <li>• PLANNED: the CPE in the service is planned, but not yet active</li> </ul>

### Prerequisite

Before using this procedure, obtain the work order or circuit detail record that contains all the parameters required to completely provision the service, including all NEs and interfaces.

The Provider Edge (PE) device must be under management by Network Integrity and the NE must be data mined prior to the service creation. The Customer Premise Equipment (CPE) device can be pre-provisioned before they are installed and brought under management.

1. [“Display the Manage Ethernet Services window” on page 107.](#)

2. Click **Create > DIA**.

The create window opens for the selected service.

3. Complete the fields as described in [“DIA values” on page 112.](#)

To select NEs and interfaces, see [“Search for an NE or interface and select it” on page 109.](#)

4. When you are satisfied with the contents, click **Apply**.

A progress window indicates the status the operation. If an error is detected, follow the instruction to correct it. To close the progress window, click **Ok**.

The following is an example DIA BGP service.

**Service Information**

Customer Name	NTWCDIA2		
Circuit ID	1402	VLAN ID	1402
Bandwidth	30	mbit/s	
State	Active	Last Updated	Thu Jul 18 18:29:46 EDT 2013, by psoundar

**DIA Type**

Type	BGP				
Customer ASN	1402	Import Policy	NTWCDIA2_AS1402		
IPv4 Customer Subnet	203.3.110.0/20	<input checked="" type="checkbox"/> Export	IPv6 Customer Subnet	2001:db8:1:0:0:0:0:48	<input checked="" type="checkbox"/> Export
PE Interface IPv4 Address	198.3.100.2/30		PE Interface IPv6 Address	2001:db8:4:4:0:0:f:2/127	
IPv4 BGP Peer	198.3.100.3		IPv6 BGP Peer	2001:db8:4:4:0:0:f:3	
IPv4 BGP Group	NTWCDIA2_AS1402_v4		IPv6 BGP Group	NTWCDIA2_AS1402_v6	

**Export Policies**

IPv4 Export Policy 1	LOCAL-ROUTES	IPv6 Export Policy 1	LOCAL-ROUTES
IPv4 Export Policy 2	DEFAULT-ROUTE	IPv6 Export Policy 2	DEFAULT-ROUTE

**Endpoint**

Customer Address	65 Hines Road, Ottawa, Ontario, K2K 4M5
<b>Provider Edge (PE)</b>	
Network Element	LAB-MX480-03
Interface	ge-0/0/5
Description	CUST:DIA:NTWCDIA2@65 Hines Road, Ottawa, Ontario, K2K 4M5:1402:

**Customer Premises Equipment (CPE)**

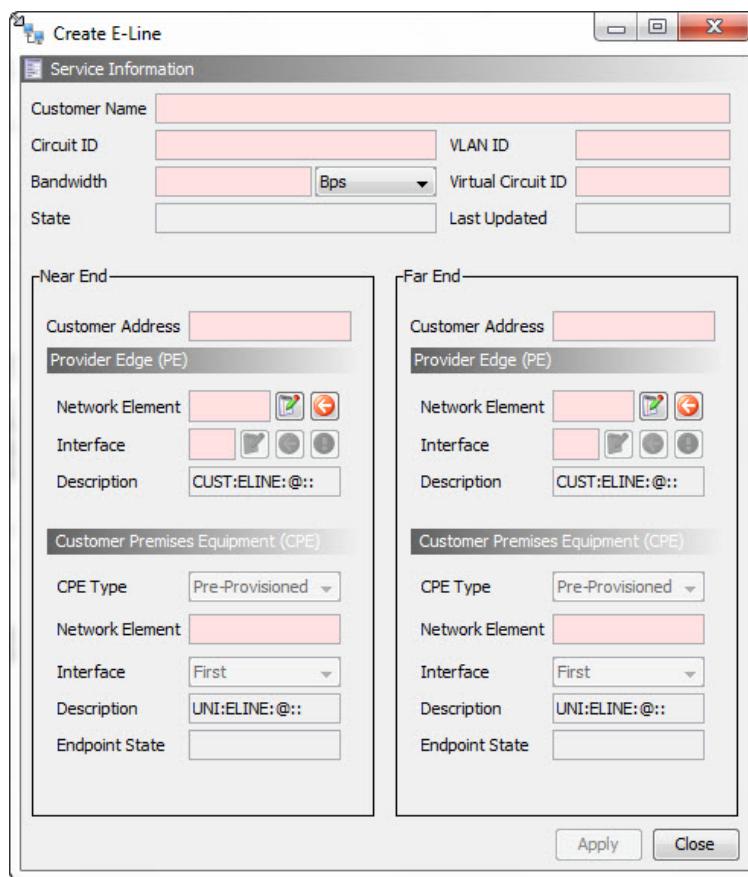
Network Element	LAB-ADVA825-06	
Interface	e100-lan-1	
Description	UNI:DIA:NTWCDIA2@65 Hines Road, Ottawa, Ontario, K2K 4M5:1402:	<input type="checkbox"/> Discovered
Endpoint State	Active	<a href="#">Activation Details...</a>

[Close](#)

## 11.4 Create an E-Line service

Use this procedure to create an E-Line service.

The following figure shows the create E-Line service dialog box.

**Figure 11–2: E-Line dialog box**

The following table explains the E-line values.

**Table 11–2: E-Line values**

Field	Description
<b>Service Information</b>	
Customer Name	The name of the customer for the service.
Circuit ID	The identifier for this network connection.
VLAN ID	The numeric identifier for the VLAN used by the service.
Bandwidth	The bandwidth measurement for the service: Bps, Kbps, Mbps, Gbps, or Tbps.
State	<p>The overall state of the service:</p> <ul style="list-style-type: none"> <li>• ACTIVE: all devices associated with the service are configured in the network.</li> <li>• PARTIAL: one or more devices that make up the service have been configured, but there are additional devices that need to be configured to complete the service.</li> <li>• PLANNED: all CPEs in the service are pre-provisioned in the Network Integrity database but the configuration has not been sent to the network.</li> </ul>

Field	Description
Last Updated	The date and time that the service was last updated
Virtual Circuit ID	The numeric identifier for the virtual circuit used by the service.
<b>Near End / Far End</b>	
The following values appear for both the Near End and the Far End, but are described only once in this table. You must complete this information for both ends of the connection.	
Customer Address	The address of the customer site for the service.
<b>Provider Edge (PE)</b>	
This defines the equipment at the PE end of the connection.	
Network Element	The NE associated with the service. To select an NE, click the "Choose the resource" button to the right of the field and search for the NE.
Interface	The name of the interface associated with the service. To select an interface, click the "Choose the interface" button to the right of the field and search for the interface on the NE
Description	The description of the service based on the type of service, the customer address, name, and circuit ID. You cannot directly modify the description. It is updated automatically as you enter the customer name, address, and circuit ID.
<b>Customer Premises Equipment (CPE)</b>	
This defines the equipment at the CPE end of the connection. It can be pre-provisioned in advance of the equipment being installed and brought under management.	
CPE Type	<p>The type of CPE:</p> <ul style="list-style-type: none"> <li>• Pre-Provisioned: the CPE is being provisioned in advance of being brought under management and being data mined.</li> <li>• Existing: the CPE is under management and has been data mined.</li> <li>• None: no CPE associated with the service. All fields and buttons are disabled.</li> </ul>
Network Element	The CPE network element that connects to the PE equipment.
Interface	<p>The name of the interface on the CPE used to connect to the PE equipment.</p> <p>For pre-provisioned NEs, the interface names are generic: First, Second, Third, Fourth, or Fifth.</p> <p>When the NE is brought under management, the name will be updated to what they are on the NE.</p>
Description	The automatically generated description of the service being provided. You cannot directly modify the description.
Endpoint State	<p>The state of the CPE endpoint:</p> <ul style="list-style-type: none"> <li>• ACTIVE: the CPE is under management and the interface is active</li> <li>• PLANNED: the CPE in the service is planned, but not yet active</li> </ul>

## Prerequisite

Before using this procedure, obtain the work order or circuit detail record that contains all the parameters required to completely provision the service, including all NEs and interfaces.

The Provider Edge (PE) devices must be under management by Network Integrity and the NE must be data mined prior to the service creation. The Customer Premise Equipment (CPE) device can be pre-provisioned before they are installed and brought under management.

1. [“Display the Manage Ethernet Services window” on page 107.](#)

2. Click **Create > E-Line**.

The create window opens for the selected service.

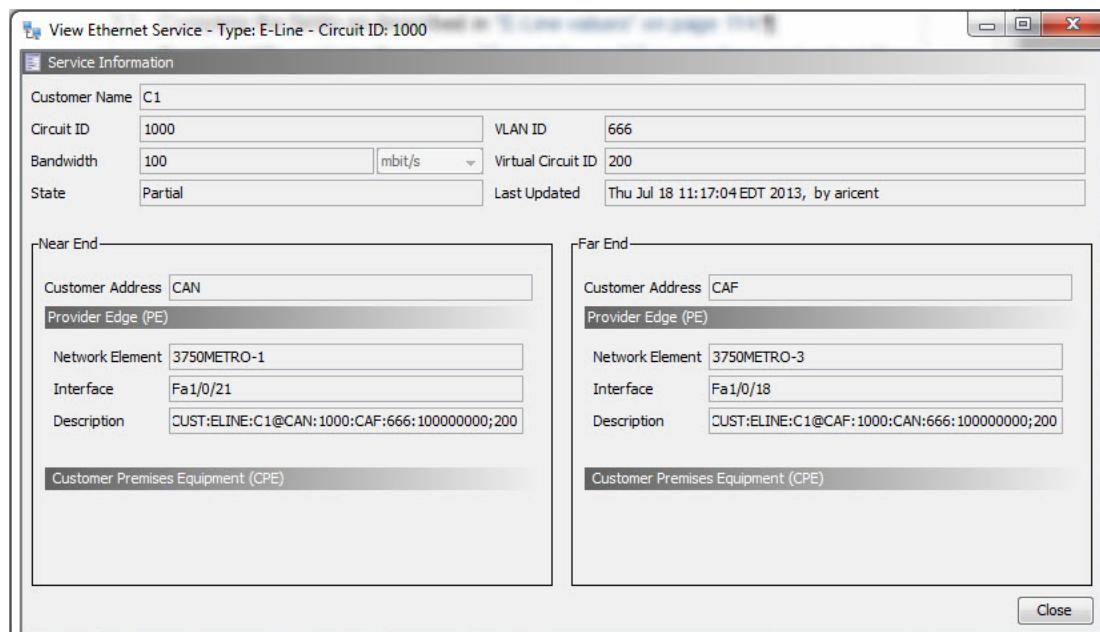
3. Complete the fields as described in [“E-Line values” on page 117.](#)

To select NEs and interfaces, see [“Search for an NE or interface and select it” on page 109.](#)

4. When you are satisfied with the contents, click **Apply**.

A progress window indicates the status the operation. If an error is detected, follow the instruction to correct it. To close the progress window, click **Ok**.

The following is an example E-Line service.



## 11.5 Create an E-LAN service

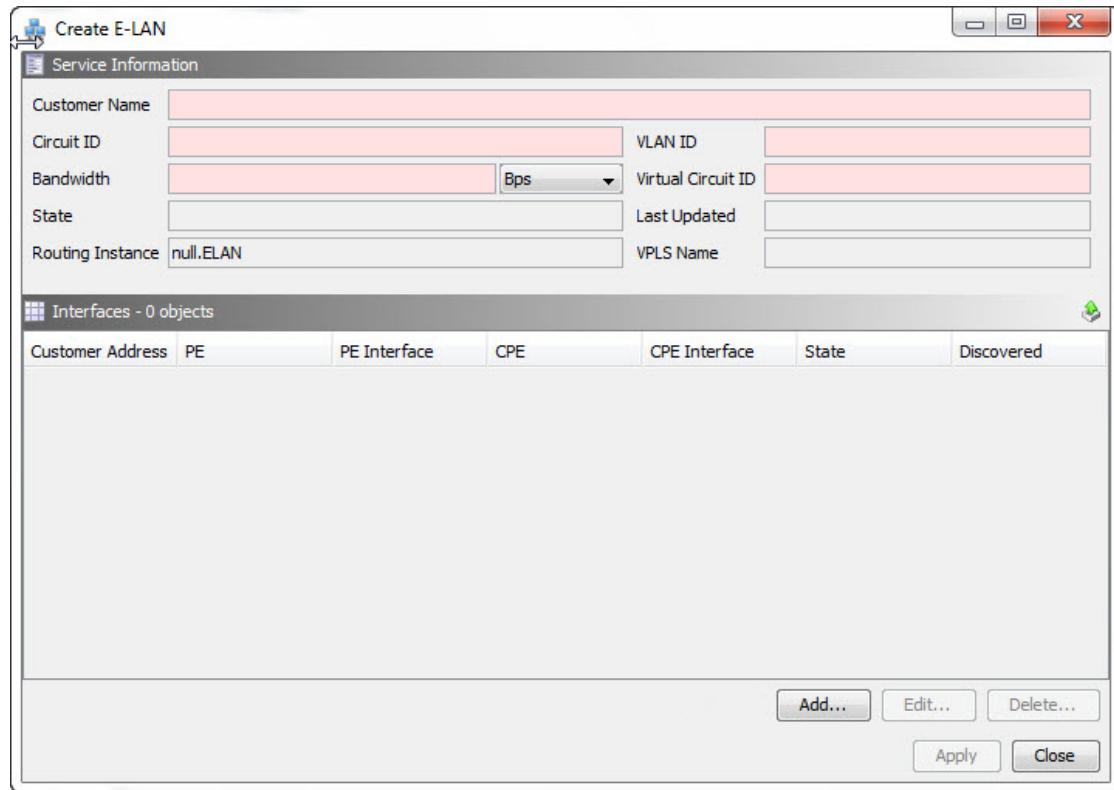
Use this procedure to create an E-LAN service.

For E-LAN services, you can provision as many nodes as are involved in the service. Each endpoint shows the attributes that must be provisioned on the PE side.

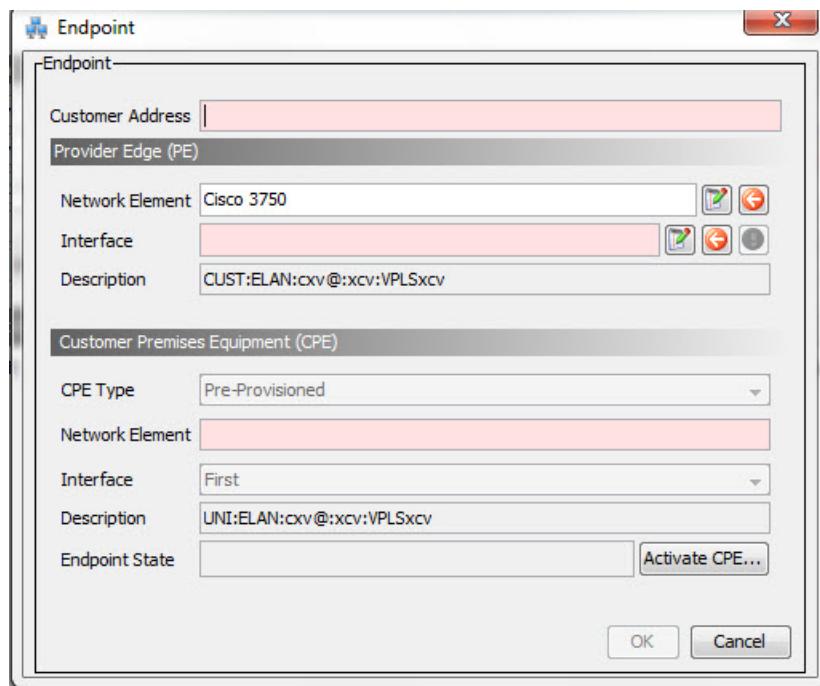
You can pre-provision the CPE endpoints in advance of the device being brought under management and data mined.

The following figure shows the create E-LAN values.

**Figure 11–3: E-LAN values**



The following figure shows the add E-LAN interface endpoint values.

**Figure 11–4: E-LAN interface endpoint values**

The following table explains the E-LAN values including the endpoints.

**Table 11–3: E-LAN values**

Field	Description
<b>Service Information</b>	
Customer Name	The name of the customer for the service.
Circuit ID	The identifier for this network connection.
VLAN ID	The numeric identifier for the VLAN used by the service.
Bandwidth	The bandwidth measurement for the service: Bps, Kbps, Mbps, Gbps, or Tbps.
State	<p>The overall state of the service:</p> <ul style="list-style-type: none"> <li>• ACTIVE: all devices associated with the service are configured in the network.</li> <li>• PARTIAL: one or more devices that make up the service have been configured, but there are additional devices that need to be configured to complete the service.</li> <li>• PLANNED: all CPEs in the service are pre-provisioned in the Network Integrity database but the configuration has not been sent to the network.</li> </ul>
Last Updated	The date and time that the service was last updated
Virtual Circuit ID	The numeric identifier for the virtual circuit used by the service.

Field	Description
Routing Instance	The routing interface name, which provides visual validation and is automatically defined as the service is created. You cannot directly modify the description.
VPLS Name	The VPLS site name, which provides visual validation and is automatically defined as the service is created. You cannot directly modify the name.
<b>Interface - Endpoint</b>	
Customer Address	The address of the customer site for the service.
<b>Provider Edge (PE)</b>	
The defines network element at the PE end of the connection.	
Network Element	The NE associated with the service. To select an NE, click the “Choose the resource” button to the right of the field and search for the NE.
Interface	The name of the interface associated with the service. To select an interface, click the “Choose the interface” button to the right of the field and search for the interface on the NE
Description	The description of the service based on the type, the customer address, name, and circuit ID. You cannot directly modify the description. It is updated automatically as you enter the customer name, address, and circuit ID.
<b>Customer Premises Equipment (CPE)</b>	
This defines the equipment at the CPE end of the connection. It can be pre-provisioned in advance of the equipment being installed and brought under management.	
CPE Type	<p>The type of CPE:</p> <ul style="list-style-type: none"> <li>• Pre-Provisioned: the CPE is being provisioned in advance of being brought under management and being data mined.</li> <li>• Existing: the CPE is under management and has been data mined.</li> <li>• None: no CPE associated with the service. All fields and buttons are disabled.</li> </ul>
Network Element	The CPE network element that connects to the PE equipment.
Interface	<p>The name of the interface on the CPE used to connect to the PE equipment.</p> <p>For pre-provisioned NEs, the interface names are generic: First, Second, Third, Fourth, or Fifth. When the NE is brought under management, the name will be updated to what they are on the NE.</p>
Description	The automatically generated description of the service being provided. You cannot directly modify the description.
Endpoint State	<p>The state of the CPE endpoint:</p> <ul style="list-style-type: none"> <li>• ACTIVE: the CPE is under management and the interface is active</li> <li>• PLANNED: the CPE in the service is planned, but not yet active</li> </ul>

1. “Display the Manage Ethernet Services window” on page 107.
2. Click **Create > E-LAN**.  
The create window opens for the selected service.
3. Complete the fields as described in “E-LAN values” on page 121.  
To select NEs and interfaces, see “Search for an NE or interface and select it” on page 109.
4. Add the interfaces that make up the E-LAN:
  - a. Click **Add**.
  - b. The Endpoint dialog box opens.
  - c. Complete the fields as described in “E-LAN values” on page 121.
  - d. When completed, click **OK**.  
The interface is added to the list.
  - e. To add more interfaces, repeat from Step a
  - f. To remove an interface, select the interface in the list and click **Remove**.
5. To modify an interface, select the interface, click **Modify**, change any values as described in “E-LAN values” on page 121 and then click **Modify**.
6. When you are satisfied with the configuration, click **Apply**.

A progress window indicates the status the operation. If an error is detected, follow the instruction to correct it. To close the progress window, click **Ok**.

The following is an example E-LAN service.

**View Ethernet Service - Type: E-LAN - Circuit ID: 201**

Service Information			
Customer Name	Waqas20		
Circuit ID	201	VLAN ID	201
Bandwidth	45	mbit/s	
State	Active	Virtual Circuit ID	201
Routing Instance	Waqas20.ELAN	VPLS Name	Waqas20

**Interfaces - 1 objects**

Customer Address	PE	PE Interface	CPE	CPE Interface	State	Discovered
Waqas20st	3750METRO-1	Fa1/0/24	FSP150CC-825	e100-lan-1	Active	X

**Activation Details...**

**Close**

## 11.6 Create an E-Tree service

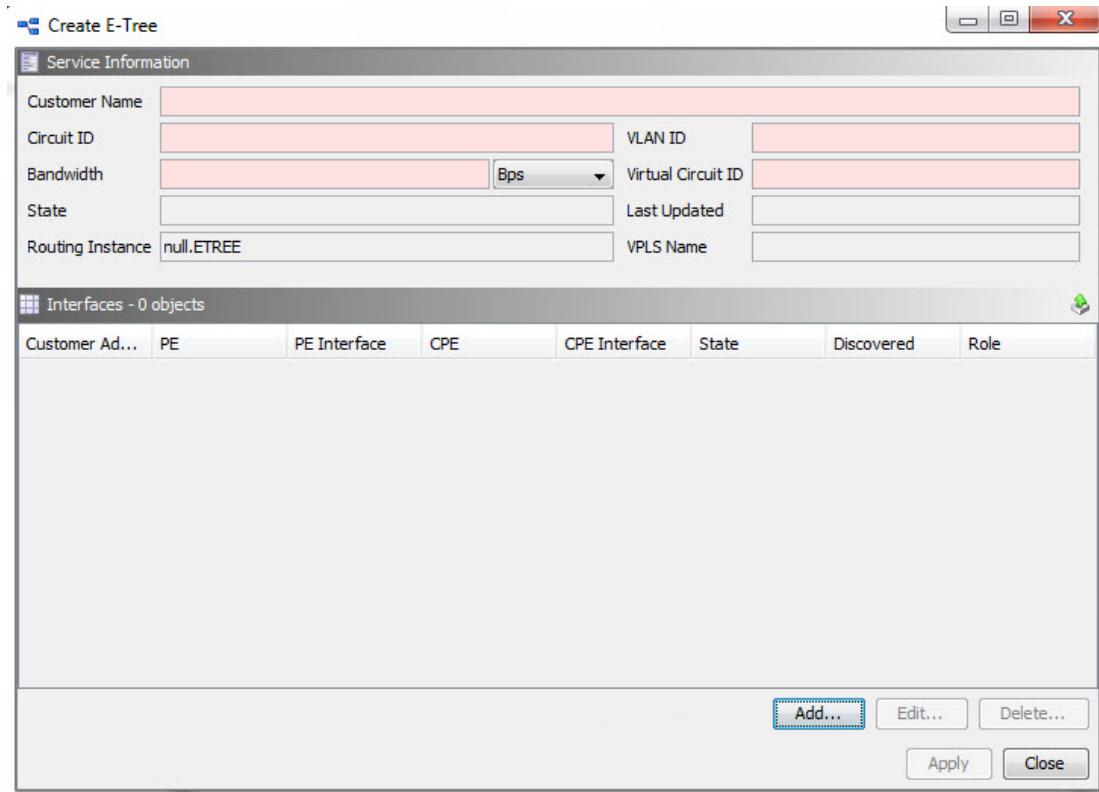
Use this procedure to create an E-Tree service.

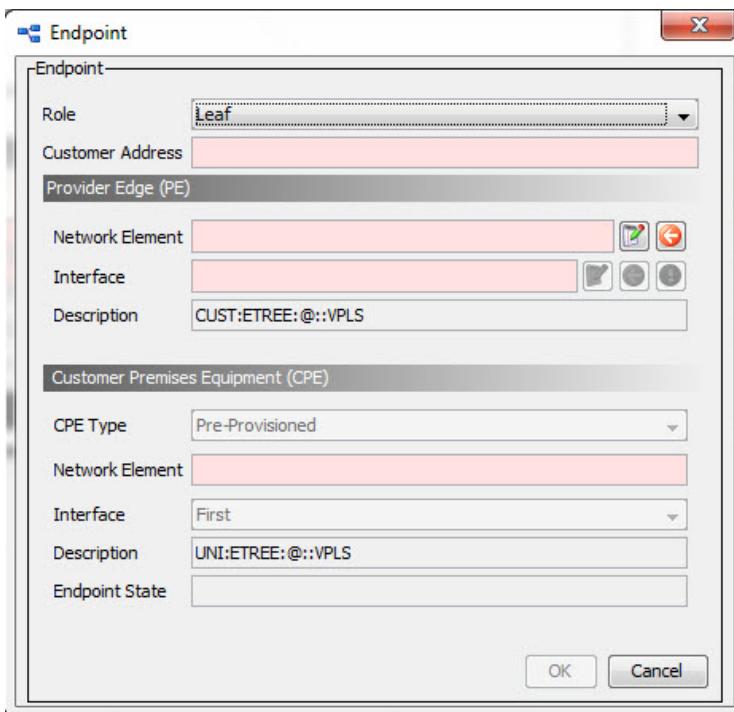
For E-Tree services, you can identify the root endpoint of the tree on the PE side. Multi-root E-Trees are supported.

You can pre-provision the CPE endpoints in advance of the device being brought under management and data mined.

The following figures show the create E-Tree values.

**Figure 11–5: E-Tree values**



**Figure 11–6: E-Tree Interface Endpoints**

The following table explains the E-Tree values.

**Table 11–4: E-Tree values**

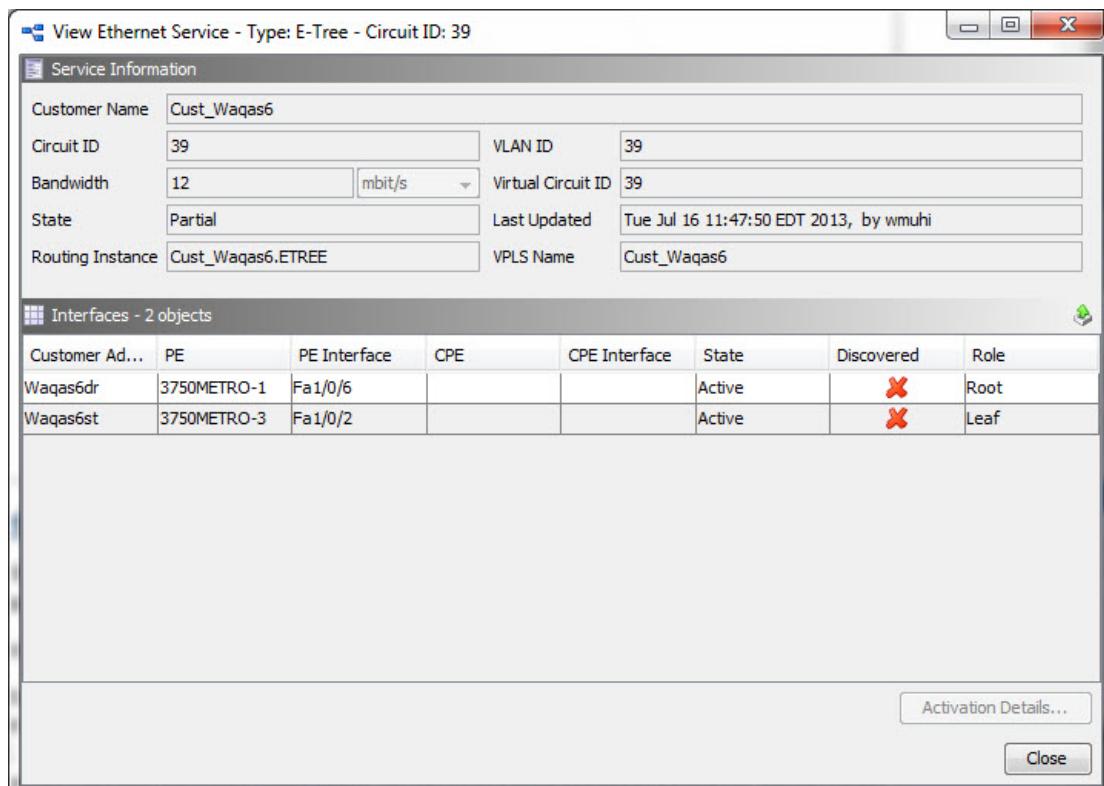
Field	Description
<b>Service Information</b>	
Customer Name	The name of the customer for the service.
Circuit ID	The identifier for this network connection.
VLAN ID	The numeric identifier for the VLAN used by the service.
Bandwidth	The bandwidth measurement for the service: Bps, Kbps, Mbps, Gbps, or Tbps.
State	<p>The overall state of the service:</p> <ul style="list-style-type: none"> <li>• ACTIVE: all devices associated with the service are configured in the network.</li> <li>• PARTIAL: one or more devices that make up the service have been configured, but there are additional devices that need to be configured to complete the service.</li> <li>• PLANNED: all CPEs in the service are pre-provisioned in the Network Integrity database but the configuration has not been sent to the network.</li> </ul>
Last Updated	The date and time that the service was last updated
Virtual Circuit ID	The numeric identifier for the virtual circuit used by the service.

Field	Description
Routing Instance	The routing interface name, which provides visual validation and is automatically defined as the service is created. You cannot directly modify the description.
VPLS Name	The VPLS site name, which provides visual validation and is automatically defined as the service is created. You cannot directly modify the name.
<b>Interface - Endpoint</b>	
Role	The role for the endpoint: Leaf or Root
Customer Address	The address of the customer site for the service.
<b>Provider Edge (PE)</b>	
The defines network element at the PE end of the connection.	
Network Element	The NE associated with the service. To select an NE, click the “Choose the resource” button to the right of the field and search for the NE.
Interface	The name of the interface associated with the service. To select an interface, click the “Choose the interface” button to the right of the field and search for the interface on the NE
Description	The description of the service based on the type, the customer address, name, and circuit ID. You cannot directly modify the description. It is updated automatically as you enter the customer name, address, and circuit ID.
<b>Customer Premises Equipment (CPE)</b>	
This defines the equipment at the CPE end of the connection. It can be pre-provisioned in advance of the equipment being installed and brought under management.	
CPE Type	<p>The type of CPE:</p> <ul style="list-style-type: none"> <li>• Pre-Provisioned: the CPE is being provisioned in advance of being brought under management and being data mined.</li> <li>• Existing: the CPE is under management and has been data mined.</li> <li>• None: no CPE associated with the service. All fields and buttons are disabled.</li> </ul>
Network Element	The CPE network element that connects to the PE equipment.
Interface	<p>The name of the interface on the CPE used to connect to the PE equipment.</p> <p>For pre-provisioned NEs, the interface names are generic: First, Second, Third, Fourth, or Fifth. When the NE is brought under management, the name will be updated to what they are on the NE.</p>
Description	The automatically generated description of the service being provided. You cannot directly modify the description.

Field	Description
Endpoint State	<p>The state of the CPE endpoint:</p> <ul style="list-style-type: none"> <li>• ACTIVE: the CPE is under management and the interface is active</li> <li>• PLANNED: the CPE in the service is planned, but not yet active</li> </ul>

1. [“Display the Manage Ethernet Services window” on page 107.](#)
2. Click **Create > E-Tree**.  
The create window opens for the selected service.
3. Complete the fields as described in “E-Tree values” on page 125.  
To select NEs and interfaces, see “Search for an NE or interface and select it” on [page 109](#).
4. Add the interfaces that make up the E-Tree:
  - a. Click **Add**.
  - b. The Endpoint dialog box opens.
  - c. Complete the fields as described in “E-Tree values” on page 125.
  - d. When completed, click **OK**.  
The interface is added to the list.
  - e. To add more interfaces, repeat from Step a.
  - f. To remove an interface, select the interface in the list and click **Remove**.
5. To modify an interface, select the interface, click **Modify**, change any values as described in “E-Tree values” on page 125 and then click **Modify**.
6. When you are satisfied with the configuration, click **Apply**.  
A progress window indicates the status the operation. If an error is detected, follow the instruction to correct it. To close the progress window, click **Ok**.

The following is an example E-Tree service.



## 11.7 Activate a pre-provisioned CPE

Use this procedure to automatically activate a CPE that was previously pre-provisioned as part of an Ethernet Service, and is now physically installed and turned up.

Activation means that the NE is brought fully under management by Network Integrity.



**CAUTION:** The activation process deletes the manufacturer default credentials from the NE. Make sure to keep a record of the passwords of other credentials you use so that you don't get locked out of the NE.

During activation, detailed logs are displayed which indicate each step of the activation process. If a step in the activation fails, you can leave the activation, correct the condition, then return to the activation and it will take over from where it left off. This can be repeated as many times as necessary until the activation succeeds. For example, if you don't have a file server configured, the log indicates that condition and you can go and configure the file server, then return to the activation.

The log will be empty for CPEs for which activation has not been attempted, or for CPEs that became active by some other means than CPE activation.

### Prerequisites

Before you can activate a pre-provisioned CPE, the following prerequisite conditions must be met:

- The CPE NE must be pre-provisioned as part of the Ethernet Service.
- The CPE NE must be physically connected to the specified provider edge (PE) NE port, and the link between them must be operationally active.
- The CPE NE is set to its factory default configuration when the CPE activation is initiated.

CPE activation uses a number of features of the NI-Framework, which must be performed before you can activate a pre-provisioned CP, as follows:

- The appropriate adapter must be installed for each type of CPE to be activated. To install an adapter, use the NI-Director administration desktop and select Nakina > Administration > Adapter Manager. For details, see the Network Integrity Framework Configuration Guide or online help.
- For initial communication with the CPE NE, the activation process will log into the CPE using the vendor default credentials. For this purpose, two Network Integrity management credential entries will be automatically created for each CPE NE unless shared management credentials are set up for the entire system (one each for CLI and SNMP).

For a shared management credential to be used by CPE activation it must meet the following naming convention:

- <adapter-name>-<interface-name> for example, for the CLI interface on the Adva 825 adapter, the management credential entry would need to be named "Adva FSP150CC-825 v2.1-CLI"

To create shared Management Credentials, use the NI-Director administration desktop and select Nakina > Administration > NE Manager, and click the Manage Credentials button. For details, see the Network Integrity Framework Management Guide or online help.

- Vendor configuration files must be imported into Network Integrity. For a given adapter, there should be one vendor configuration file for each supported common CPE configuration. For example, if the common CPE configuration varies by region, there should be one common vendor configuration file per adapter, per region; such as:
  - "EasternRegion" (Adva 825)
  - "EasternRegion" (Adva 114)
  - "EasternRegion" (RAD 205)
  - "WesternRegion" (Adva 825)

These configuration files should not manipulate CLI user ids or SNMP community names. These will be managed using NE security templates.

To create vendor configuration files, use the NI-Director administration desktop and select the Vendor Files tool. For details, see the NI-Director User Guide or online help.

- Dynamic NE groups must be created to automatically contain the CPEs as they are activated. The names of these dynamic NE groups must exactly match the names of the vendor configuration files created in the previous step. For example, if vendor configuration files called "EasternRegion" have been created for each CPE adapter type, a single dynamic group called "EasternRegion" should be created to hold all Eastern region CPEs. The containment specification of the dynamic group is specific and dependent on the customer's CPE NE naming convention. For example, if all Eastern region CPEs have the word 'East' embedded in their names, the dynamic group specification could be "\*East\*".

An activating CPE must be contained by only one dynamic group that has the same name as a vendor configuration file. The CPE activation process uses the name of the containing dynamic group to determine the appropriate vendor file to apply,

which is why there should be only one. The NE can be contained in other dynamic groups as long as those groups have no corresponding vendor configuration file.

To create dynamic NE groups, use the NI-Director administration desktop and select Nakina > Administration > NE Group Manager. For details, see the Network Integrity Framework Configuration Guide or online help.

- A managed file server with the following characteristics must be defined in the Network Integrity database to be used for transferring the vendor-specific configuration files to the CPEs during activation:
  - The file server must be defined as 'Remote'.
  - The file server administrative state must by 'Unlocked'.
  - The file server must contain a directory called "activation" in the user's home directory on the server, such as /export/home/user.
  - All CPEs to be activated must be able to connect to the file server to pull the vendor configuration file.
  - The file server must support the file transfer protocol(s) that the CPEs use to pull configuration files.
  - If different CPE types use different transfer protocols, one file server for each protocol must be defined, for example, one for FTP, one for SFTP, etc.
  - If there is more than one remote file server in the system that meets the above requirements for a given CPE being activated, CPE activation will use the remote file server that is alphabetically first by name.

To create a managed file server, use the NI-Director administration desktop and select Nakina > Administration > File Server. For details, see the Network Integrity Framework Configuration Guide or online help.

- NE security templates with the following characteristics must be defined with the credentials to be configured on the CPEs as part of the activation:
  - The name of the NE security template must exactly match the adapter name of the CPE being activated, for example, "Adva FSP150CC-825 v2.1").
  - There should be one NE security template created for each CPE adapter type used by CPE activation.
  - The NE security template should contain all CLI user ids and SNMP community names to be provisioned on the CPE.
  - The NE security template must specify one CLI user id and one SNMP community name as the management credentials to be used by Network Integrity.
  - The NE security template must not contain any of the vendor default CLI user ids and SNMP community strings. These default credentials are automatically deleted from the CPE as part of the CPE activation and therefore must not be referenced by the NE security template.

To create NE security templates, use the NI-Director administration desktop and launch the NE Security Template tool on the desktop. For details, click "?" in the NE Security Template window.

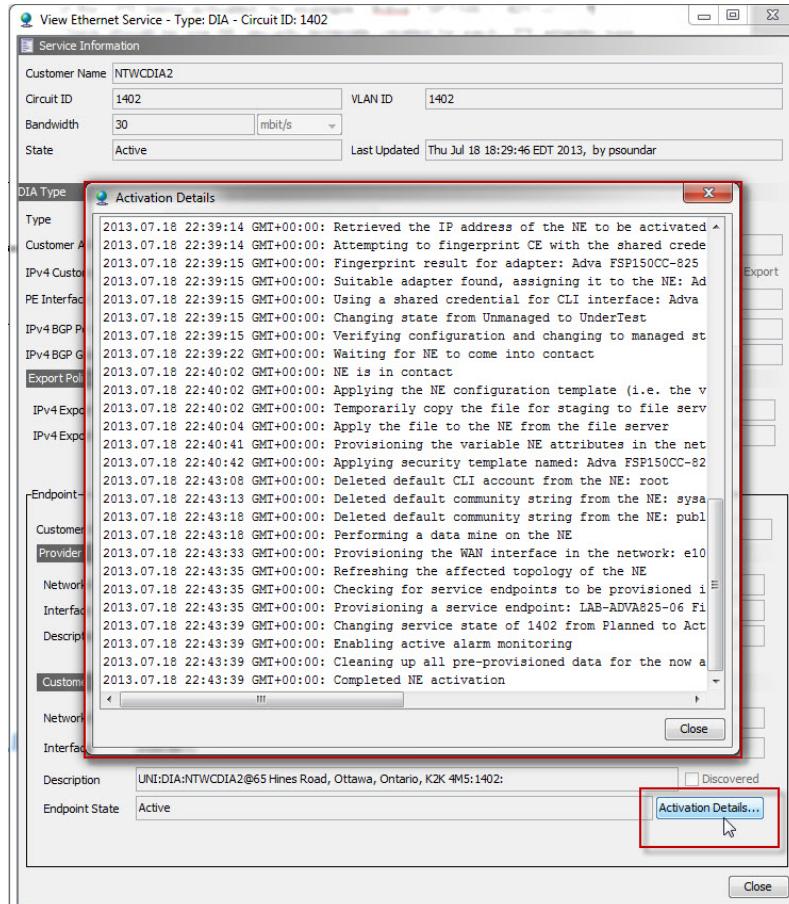
1. ["Display the Manage Ethernet Services window" on page 107.](#)
2. Click **View** and select the service (**DIA**, **E-LINE**, **E-LAN**, or **E-Tree**).  
The view window opens for the selected service.
3. Beside the desired CPE, click **Activation Details**.

The Activation Details window appears. If this is the first attempt at activation, the window is blank, but if this is a subsequent attempt, the previous details are displayed.

#### 4. Click **Activate CPE**.

The Activation Details window displays the progress of the activation. If a step in the activation fails, correct the condition, then return to this window and click **Activate CPE** to resume the activation. You can repeat the activation as many times as required until the activation is successful.

When the activation succeeds, the buttons will no longer be visible, and the final message will be "Completed NE Activation"..



#### 5. To close the details window, click **Close**.

After activation, the service state is updated automatically in the "View Ethernet Service" window.

## 11.8 Modify an ethernet service

To modify an ethernet service, use the procedure to create a service of the same name which will overwrite the service with the revised parameters.

### To modify CPE information:

1. Click **View** and select the service (**DIA**, **E-LINE**, **E-LAN**, or **E-Tree**).  
The view window opens for the selected service.
2. Beside the desired CPE, click **Activation Details**.  
The Activation Details window appears.
3. Click **Modify CPE**.
4. Enter a new name for the CPE NE and click OK.

### To delete CPE information:

1. Click **View** and select the service (**DIA**, **E-LINE**, **E-LAN**, or **E-Tree**).  
The view window opens for the selected service.
2. Beside the desired CPE, click **Activation Details**.  
The Activation Details window appears.
3. Click **Delete CPE**.  
The system prompts for confirmation.
4. To confirm the deletion, click Yes. To cancel the deletion, click No.

# 12 Configuring and using Ethernet OAM

This section explains how to configure and use Ethernet operations, administration, and maintenance (OAM). It contains the following sub-sections:

- “How to obtain more information about Ethernet OAM fields” on page 133
- “Configuring and using link fault management” on page 134
- “Configuring and using connectivity fault management” on page 138
- “Perform an MPLS LDP traceroute test” on page 151

This section contains only Ethernet OAM information. For general maintenance procedures, see “[Performing maintenance](#)” on page 84.



**Note:** The images shown in this chapter are examples only. The actual fields will be different depending on the type of NE and adapter that you are working with.

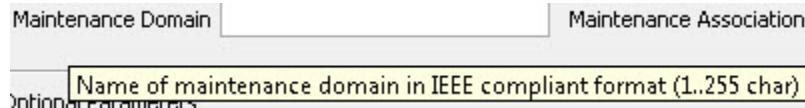


**Note:** If while using the NOC you do not see menu items, tabs or buttons that are described in this documentation, it is because the Network Integrity administrator has not assigned the permission to your user account, or the feature has not been installed.

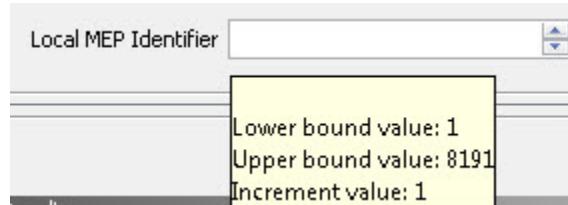
## 12.1 How to obtain more information about Ethernet OAM fields

Because the fields available in each window will differ depending on the NE and adapter, information about the fields is not provided in this chapter. To obtain more information, you can move your mouse over the fields in each Ethernet OAM window.

To get more information about the definition of a field, move the mouse over the field name, for example:



To get more information about the valid values for a field, move the mouse over the data entry field, for example:



## 12.2 Configuring and using link fault management

Link fault management (LFM) must be enabled on the interfaces at the two ends of a link for the link to be monitored.

You can retrieve and display LFM details for a given interface or all interfaces on an NE.

This section explains how to:

- “Configure link fault management” on page 134
- “View link fault management details” on page 135
- “Clear link fault management state or statistics” on page 136

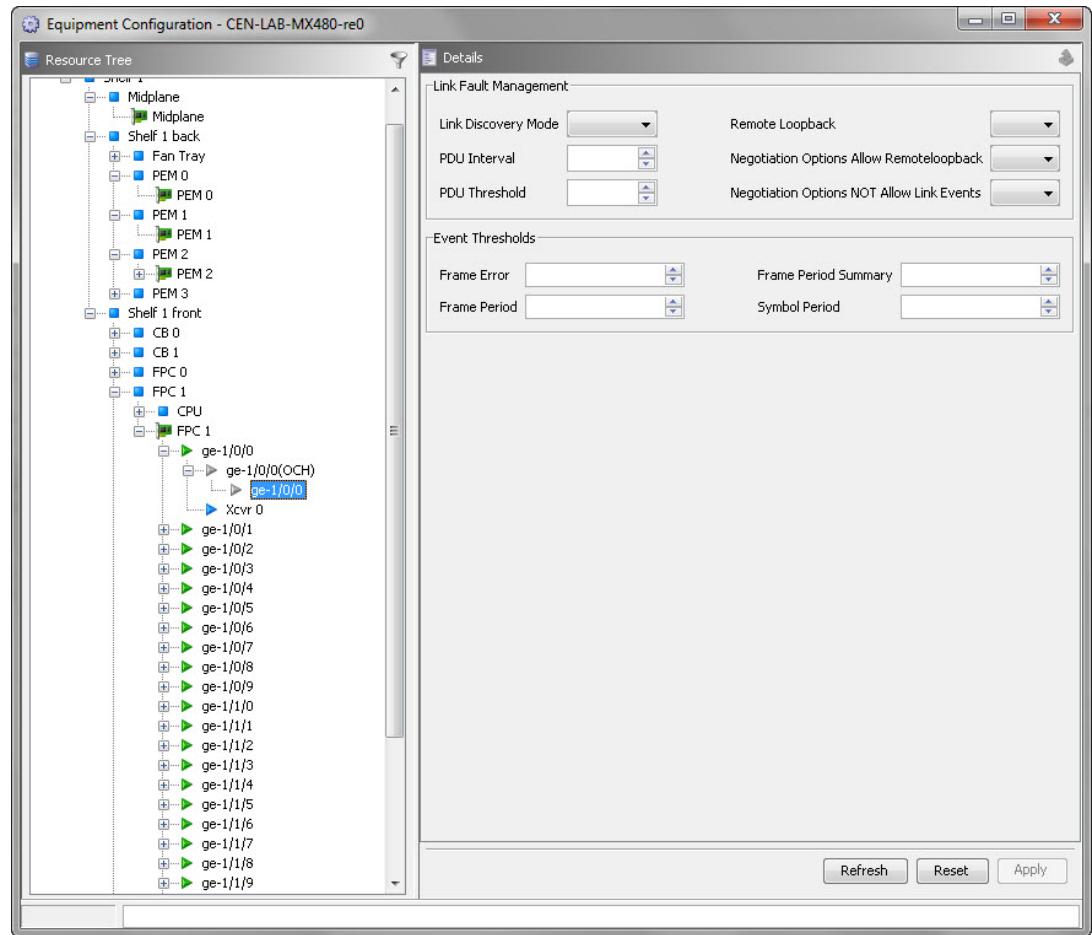
### 12.2.1 Configure link fault management

To use link fault management, you must enable link fault management on an interface and define optional parameters, for example the PDU interval.

Use this procedure to enable link fault management on an interface.

1. In the Network Element View window, navigate to the interface on which to configure link fault management, right-click, and choose **Provisioning > Equipment Configuration**.

The Equipment Configuration window opens with the link fault management information displayed, as in this example:



More information about the Equipment Configuration window is available in [“Configuring equipment” on page 53](#).

2. Mouse over the fields to obtain more information about field content and valid values.
3. Complete the fields as required and click **Apply**.

## 12.2.2 View link fault management details

Use this procedure to view raw link fault management details at the NE level or the interface level. At the NE level, information about all interfaces on the NE is provided. At the interface level, only information about that interface is provided.

1. Do one of the following:
  - To view LFM information for all interfaces on an NE, in the Network Elements table or the Topology view, right-click the NE and choose **Maintenance** → **Retrieve Information** → **Show LFM Details**.

- To view LFM information for an interface, in the Network Element View window, right-click the interface and choose **Maintenance** → **Retrieve Information** → **Show LFM Details**.

The Show LFM Details window opens, similar to the following:

```

Show LFM Details - CEN-LAB-MX240-re0

Interface: ge-1/0/0
Status: Running, Discovery state: Fault
Peer address: 00:00:00:00:00:00
Flags:0x8

Interface: ge-1/0/1
Status: Running, Discovery state: Passive Wait
Peer address: 00:00:00:00:00:00
Flags:0x8

Interface: ge-1/0/2
Status: Running, Discovery state: Fault
Peer address: 00:00:00:00:00:00
Flags:0x8

Interface: ge-1/1/2
Status: Down
{master}

interface ge-1/1/2 {
    pdu-interval 101;
    link-discovery active;
    pdu-threshold 4;
    negotiation-options {
        no-allow-link-events;
    }
}
interface ge-1/0/1 {
    link-discovery passive;
}

```

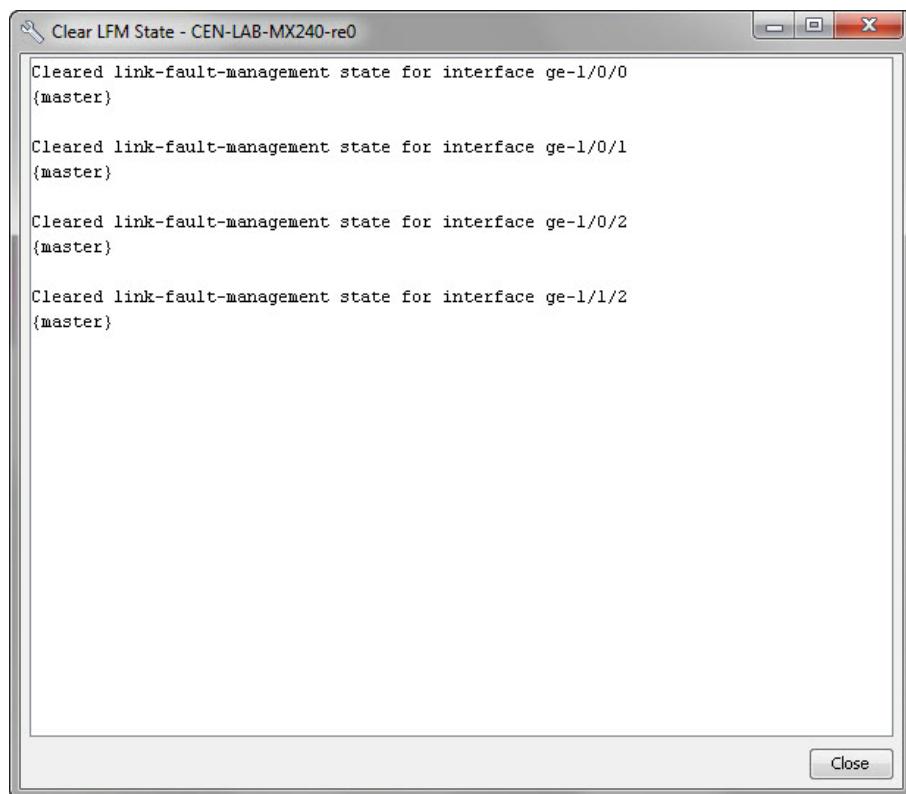
- Click **Close** to close the window,

### 12.2.3 Clear link fault management state or statistics

Use this procedure to clear link fault management state or statistic information at the NE or interface level.

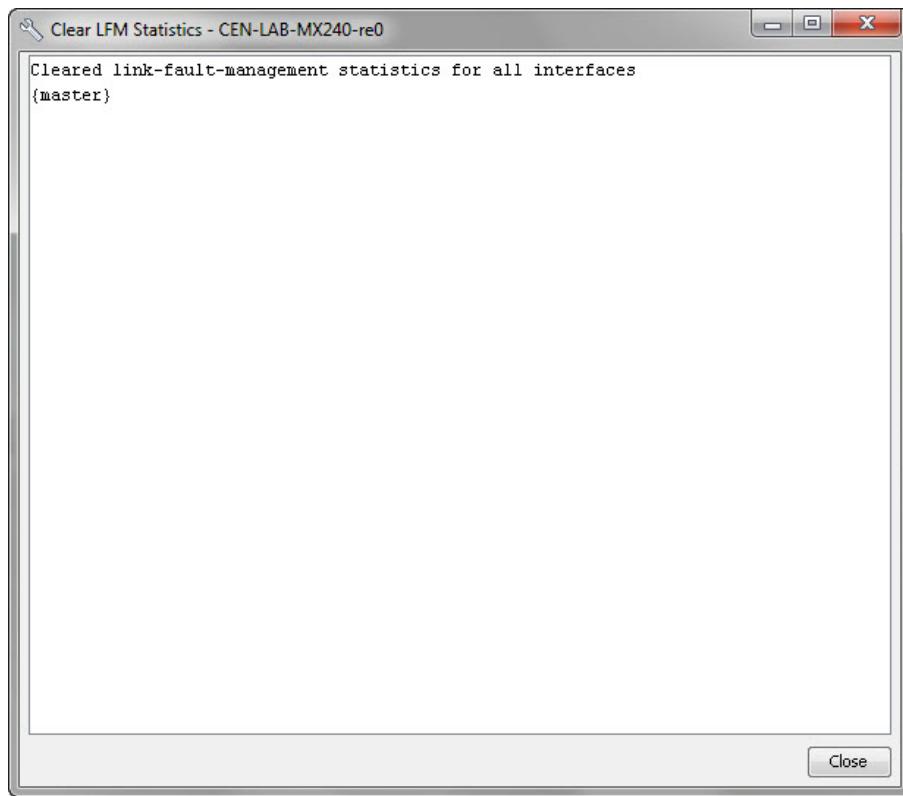
- To clear LFM state information, do one of the following:
  - To clear LFM state information for all interfaces on an NE, in the Network Elements table or the Topology view, right-click the NE and choose **Maintenance** → **Clear** → **Clear LFM State**.
  - To clear LFM state information for an interface, in the Network Element View window, right-click the interface and choose **Maintenance** → **Clear** → **Clear LFM State**.

A confirmation window is displayed, for example:



2. To clear LFM statistics, do one of the following:
  - To clear LFM statistics for all interfaces on an NE, in the Network Elements table or the Topology view, right-click the NE and choose **Maintenance** → **Clear** → **Clear LFM Statistics**.
  - To clear LFM statistics for a single interface, in the Network Element View window, right-click the interface and choose **Maintenance** → **Clear** → **Clear LFM Statistics**.

A confirmation window is displayed, for example:



3. Click **Close** to close the window.

## 12.3 Configuring and using connectivity fault management

This section contains the following sub-sections:

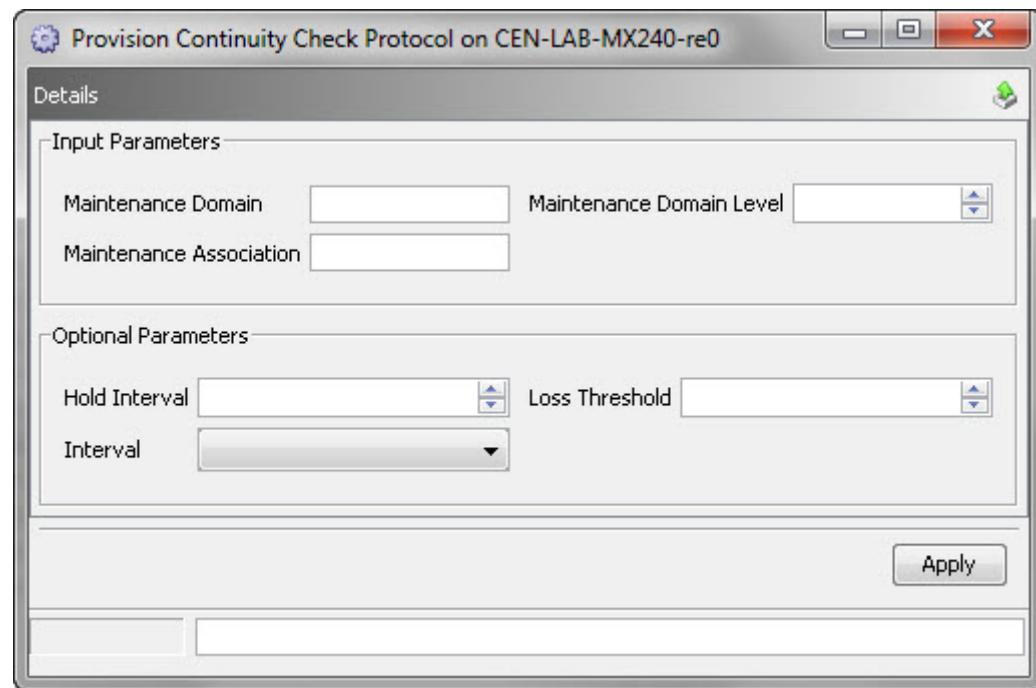
- ["Configure and use the continuity check protocol" on page 138](#)
- ["Determine connectivity using the loopback protocol" on page 139](#)
- ["Configure and use the link trace protocol" on page 140](#)
- ["View and clear CFM policer information" on page 144](#)
- ["View and clear other CFM data" on page 146](#)

### 12.3.1 Configure and use the continuity check protocol

Use this procedure to enable the continuity check protocol on the NE for continuity check messages to be automatically exchanged between its maintenance association endpoints (MEPs) and their peers in the network. The continuity check protocol is used for fault detection by a MEP.

1. in the Network Elements table or the Topology view, right-click the NE and choose **Provisioning** → **Other Resources** → **Continuity Check Protocol**.

The Provision Continuity Check Protocol window opens, for example:



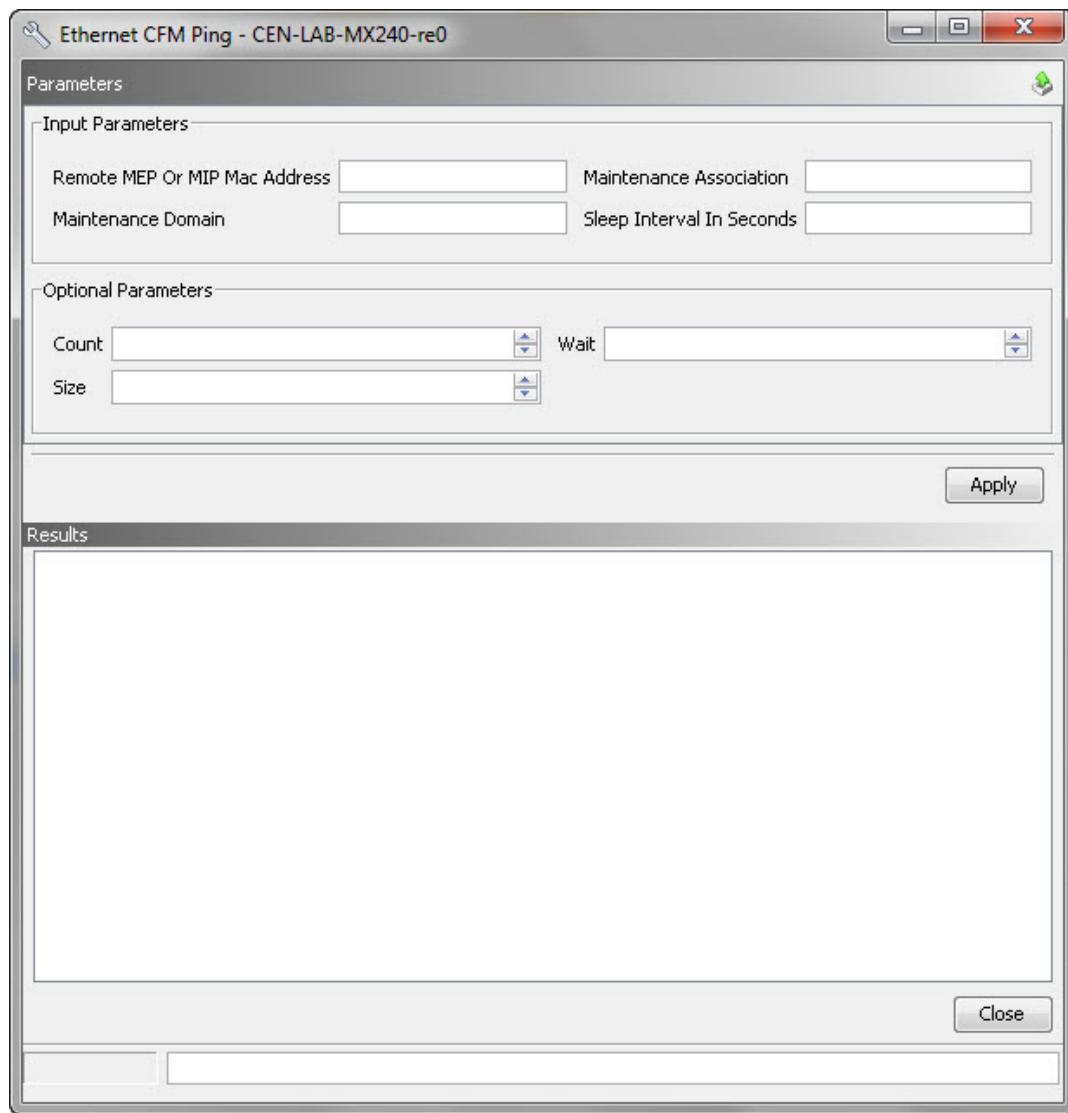
2. Define the input parameters and optional parameters in the fields provided. You can move your mouse over the fields for more information and valid values.
3. If you want to save the configuration information, you can [“Save the visible table data to a file” on page 24](#).
4. When you are satisfied with the information you entered, click **Apply**.

### 12.3.2 Determine connectivity using the loopback protocol

Use this procedure to determine whether a destination is reachable. This is done using an "Ethernet Ping" test.

1. In the Network Elements table or the Topology view, right-click the NE and choose **Maintenance** → **Test** → **Ethernet CFM Ping**.

The Ethernet CFM Ping window opens, for example:



2. Define the input parameters and optional parameters in the fields provided. You can move your mouse over the fields for more information and valid values.
3. Click **Apply**.  
The results are displayed in the Results section.
4. If you want to save the configuration information, you can “[Save the visible table data to a file](#)” on page 24.
5. When you are finished viewing the information, click **Close** to close the window.

### 12.3.3 Configure and use the link trace protocol

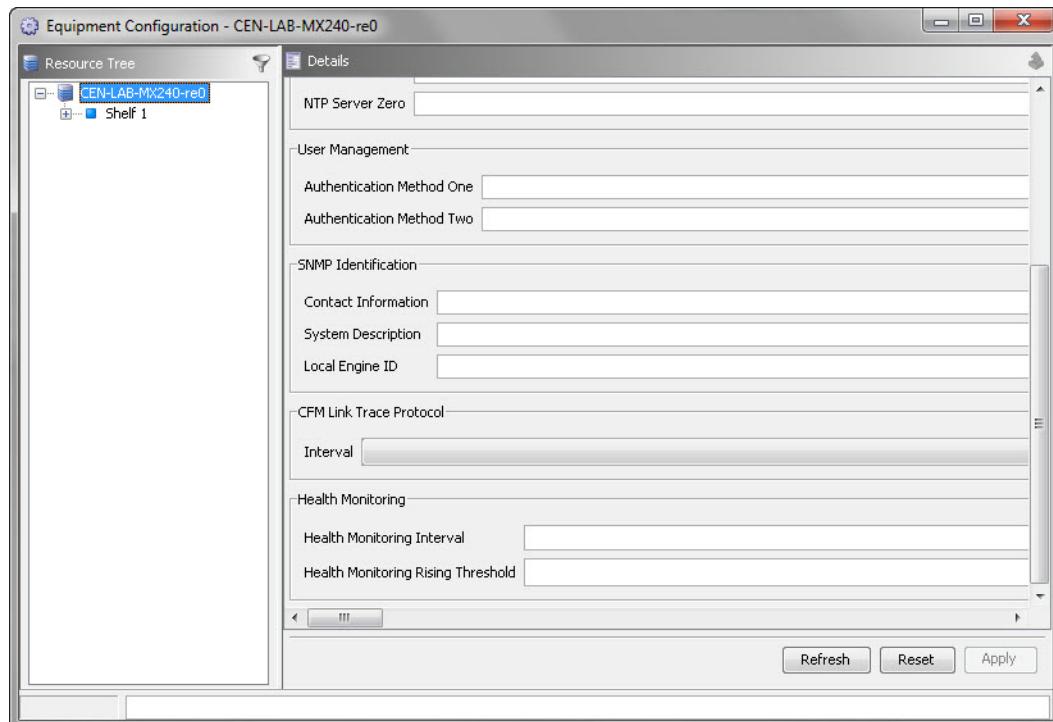
This section explains how to:

- “[Configure the link trace protocol](#)” on page 141

- “Perform an Ethernet CFM Traceroute test” on page 141
- “View CFM Path Database information” on page 142
- “Clear CFM Link Trace Path Database information” on page 143

## Configure the link trace protocol

1. In the Network Elements table or the Topology view, right-click the NE and choose **Provisioning** → **Equipment Configuration**.
2. The Equipment Configuration window opens, for example:

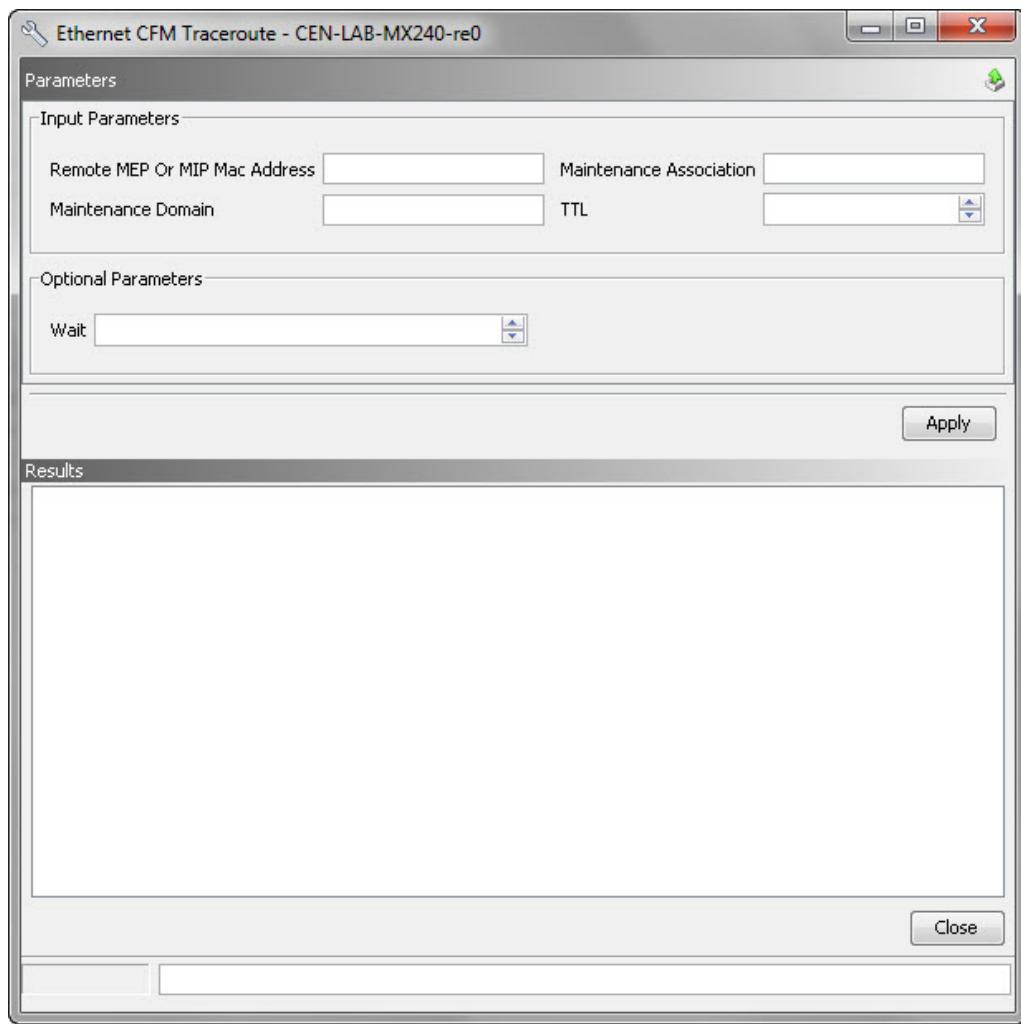


3. Complete the fields in the CFM Link Trace Protocol section.
4. Click **Apply**.

## Perform an Ethernet CFM Traceroute test

1. In the Network Elements table or the Topology view, right-click the NE and choose **Maintenance** → **Test** → **Ethernet CFM Traceroute**.

The Ethernet CFM Traceroute window opens, for example.

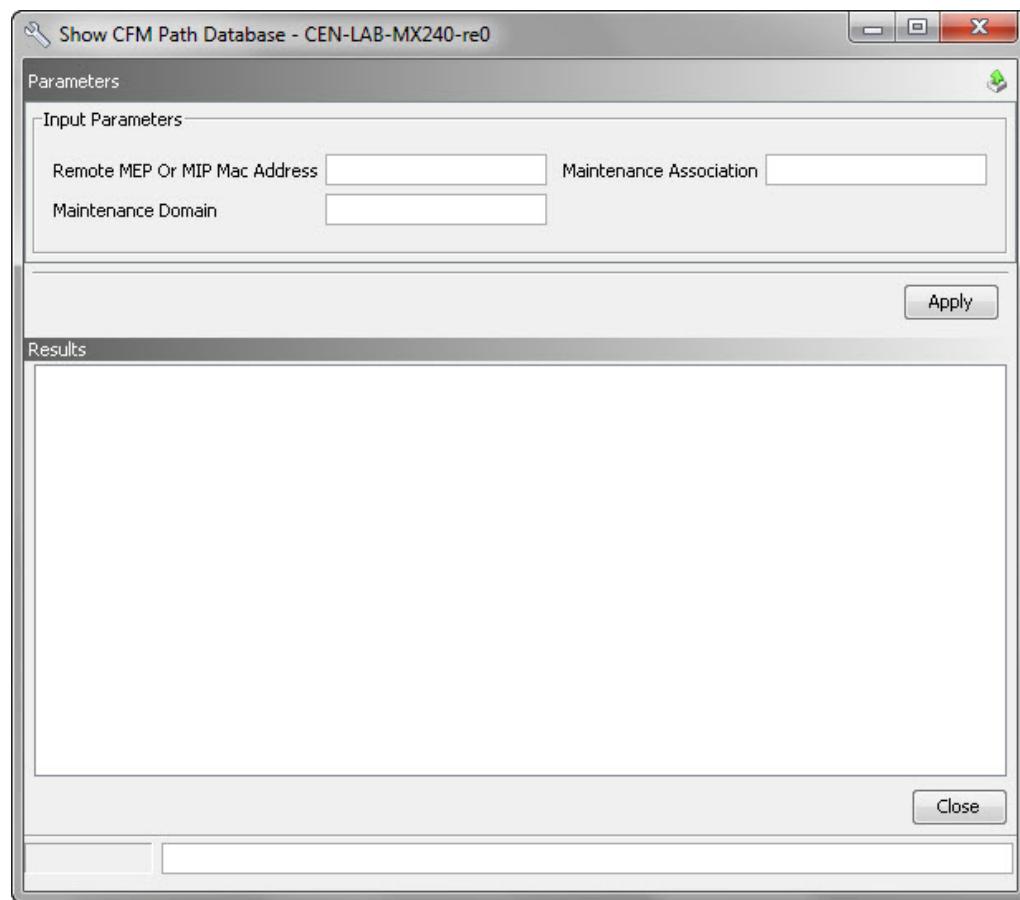


2. Define the input parameters and optional parameters in the fields provided.  
You can move your mouse over the fields for more information and valid values.
3. Click **Apply**.  
The results are displayed in the Results section.
4. If you want to save the configuration information, you can “Save the visible table data to a file” on page 24.
5. When you are finished viewing the information, click **Close** to close the window.

### **View CFM Path Database information**

1. In the Network Elements table or the Topology view, right-click the NE and choose **Maintenance** → **Retrieve Information** → **Show CFM Path Database**.

The Show CFM Path Database window opens, for example:

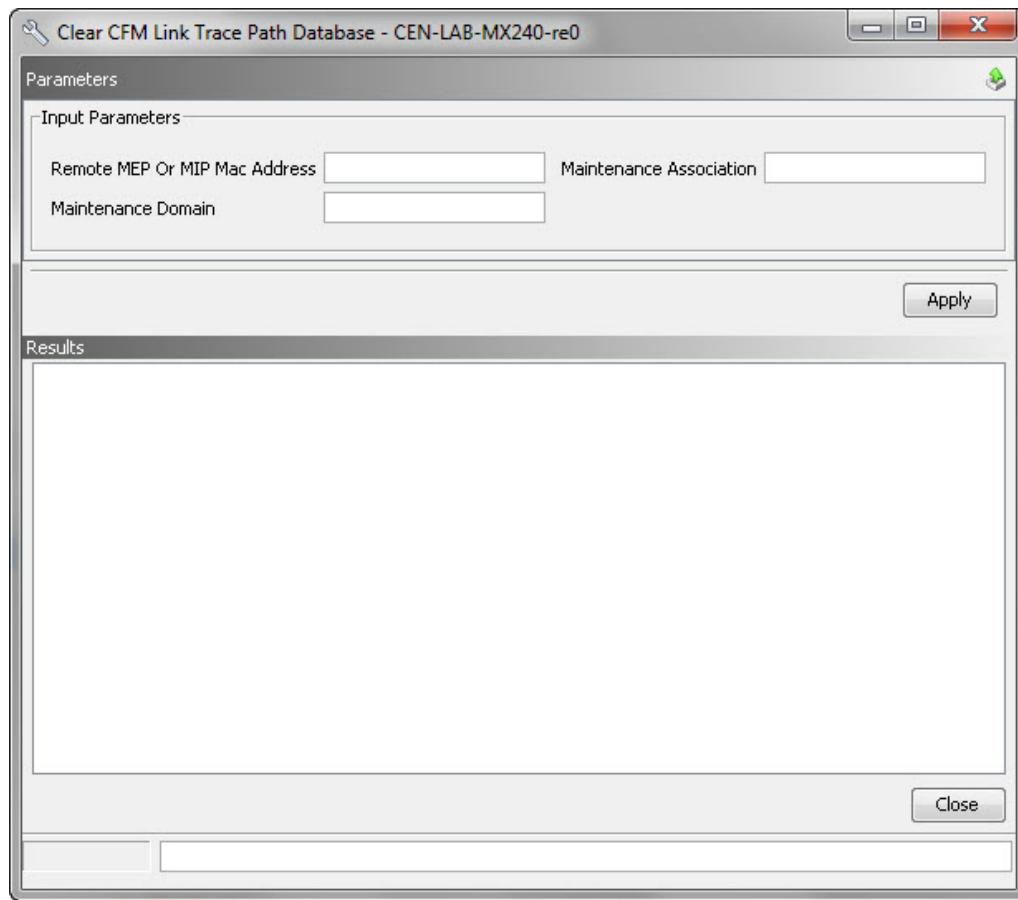


2. Define the input parameters in the fields provided.  
You can move your mouse over the fields for more information and valid values.
3. Click **Apply**.  
The information is displayed in the Results section.
4. If you want to save the configuration information, you can [“Save the visible table data to a file” on page 24](#).
5. When you are finished viewing the information, click **Close** to close the window.

### Clear CFM Link Trace Path Database information

1. In the Network Elements table or the Topology view, right-click the NE and choose **Maintenance** → **Clear** → **CFM Link Trace Path Database**.

The Clear CFM Link Trace Path Database window opens, for example:



2. Define the input parameters in the fields provided.  
You can move your mouse over the fields for more information and valid values.
3. Click **Apply**.  
The results are displayed in the Results section.
4. If you want to save the configuration information, you can “[Save the visible table data to a file](#)” on page 24.
5. When you are finished viewing the information, click **Close** to close the window.

#### 12.3.4 View and clear CFM policer information

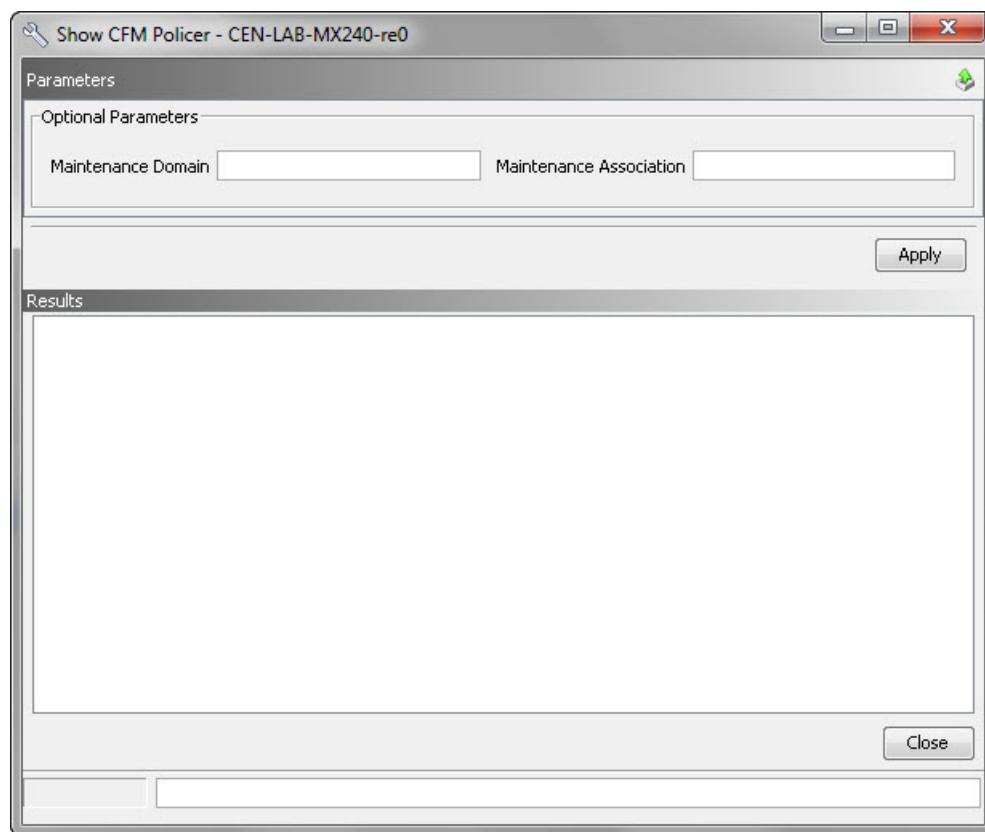
This section explains how to:

- “[View CFM Policer information](#)” on page 144
- “[Clear CFM Policer information](#)” on page 145

##### View CFM Policer information

1. In the Network Elements table or the Topology view, right-click the NE and choose **Maintenance** → **Retrieve Information** → **Show CFM Policer**.

The Show CFM Policer window opens, for example:

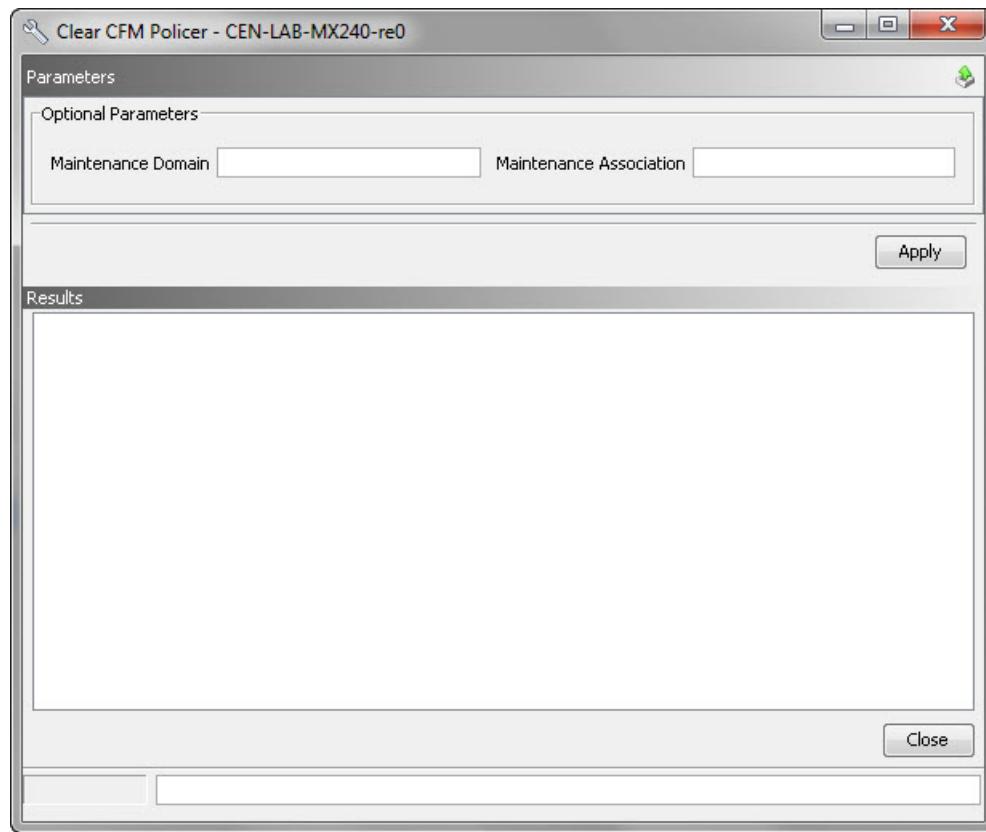


2. If you choose to, define the optional parameters in the fields provided. You can move your mouse over the fields for more information and valid values.
3. Click **Apply**.  
The information is displayed in the Results section.
4. If you want to save the configuration information, you can "[Save the visible table data to a file](#)" on page 24.
5. When you are finished viewing the information, click **Close** to close the window.

### **Clear CFM Policer information**

1. In the Network Elements table or the Topology view, right-click the NE and choose **Maintenance** → **Clear** → **CFM Policer**.

The Clear CFM Policer window opens, for example:



2. If you choose to, define the optional parameters in the fields provided.  
You can move your mouse over the fields for more information and valid values.
3. Click **Apply**.  
The results are displayed in the Results section.
4. If you want to save the configuration information, you can “Save the visible table data to a file” on page 24.
5. When you are finished viewing the information, click **Close** to close the window.

### 12.3.5 View and clear other CFM data

This section explains how to:

- “View CFM forwarding state information” on page 146
- “View CFM interfaces” on page 147
- “View CFM MEP database information” on page 149
- “View CFM MIP information” on page 149
- “Clear CFM Statistics” on page 150

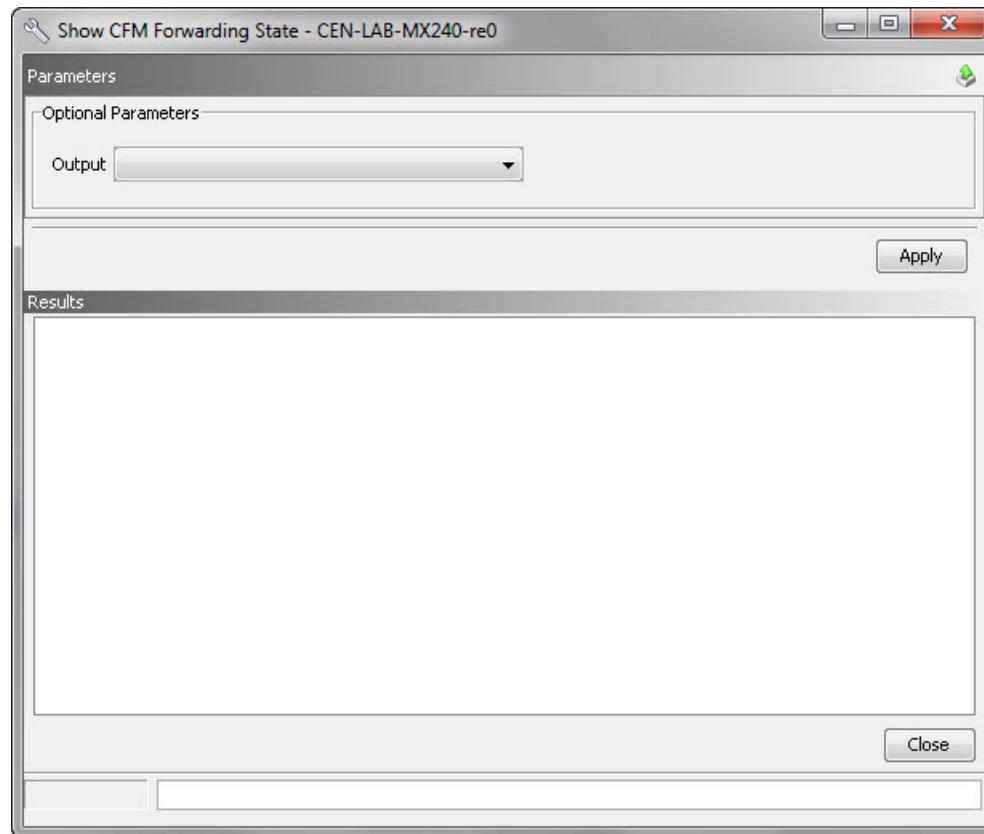
#### View CFM forwarding state information

1. Do one of the following:

- To view CFM forwarding state information at the NE level, in the Network Elements table or the Topology view, right-click the NE and choose **Maintenance** → **Retrieve Information** → **Show CFM Forwarding State**.
- To view CFM forwarding state information at the interface level, in the Network Element View window, right-click the interface and choose **Maintenance** → **Retrieve Information** → **Show CFM Forwarding State**.

The Show CFM Forwarding State window opens. The context is either the NE or the interface, depending on how the window was accessed.

For example:



2. If you choose to, define the optional parameters in the fields provided. You can move your mouse over the fields for more information and valid values.
3. Click **Apply**. The information is displayed in the Results section.
4. If you want to save the configuration information, you can “[Save the visible table data to a file](#)” on page 24.
5. When you are finished viewing the information, click **Close** to close the window.

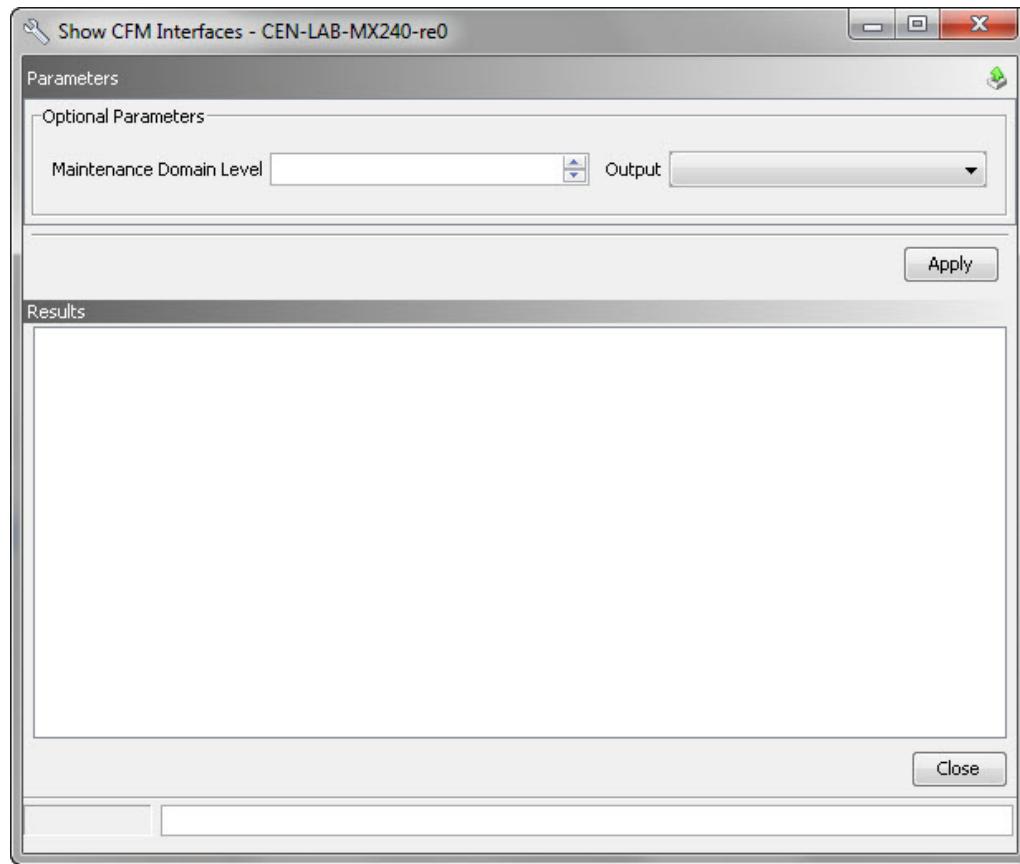
### **View CFM interfaces**

1. Do one of the following:

- To view CFM interfaces at the NE level, in the Network Elements table or the Topology view, right-click the NE and choose **Maintenance** → **Retrieve Information** → **Show CFM Interfaces**.
- To view CFM interfaces at the interface level, in the Network Element View window, right-click the interface and choose **Maintenance** → **Retrieve Information** → **Show CFM Interfaces**.

The Show CFM Interfaces window opens. The context is either the NE or the interface, depending on how the window was accessed.

For example:

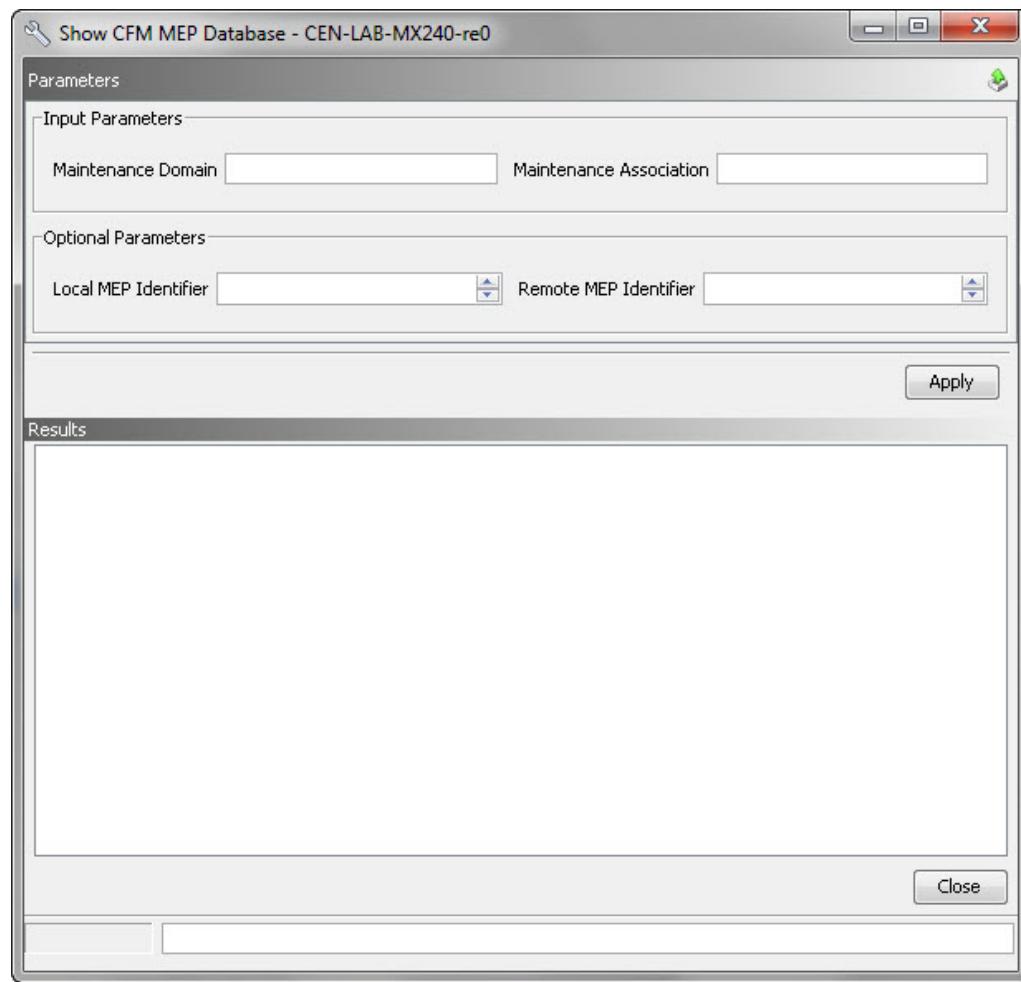


2. If you choose to, define the optional parameters in the fields provided. You can move your mouse over the fields for more information and valid values.
3. Click **Apply**.  
The information is displayed in the Results section.
4. If you want to save the configuration information, you can “Save the visible table data to a file” on page 24.
5. When you are finished viewing the information, click **Close** to close the window.

## View CFM MEP database information

1. In the Network Elements table or the Topology view, right-click the NE and choose **Maintenance** → **Retrieve Information** → **Show CFM MEP Database**.

The Show CFM MEP Database window opens, for example:

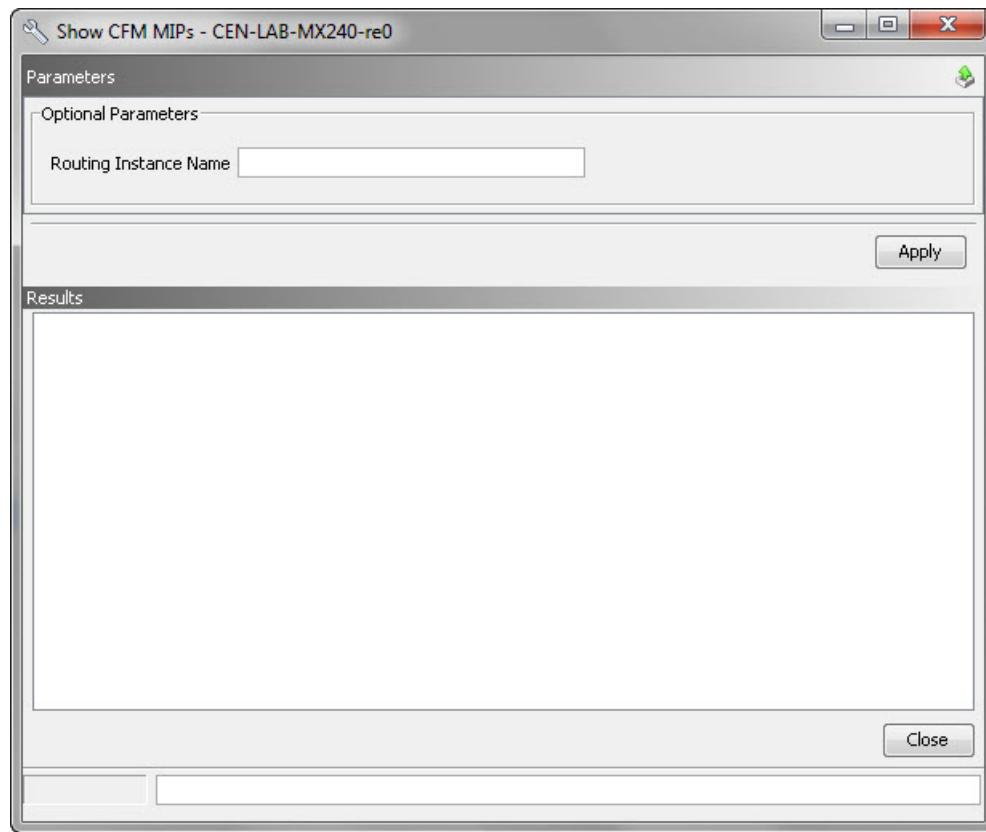


2. Define the input parameters and optional parameters in the fields provided. You can move your mouse over the fields for more information and valid values.
3. When you are satisfied with the information you entered, click **Apply**. The information is displayed in the Results section.
4. If you want to save the configuration information, you can “[Save the visible table data to a file](#)” on page 24.
5. When you are finished viewing the information, click **Close** to close the window.

## View CFM MIP information

1. In the Network Elements table or the Topology view, right-click the NE and choose **Maintenance** → **Retrieve Information** → **Show CFM MIPs**.

The Show CFM MIPs window opens, for example:



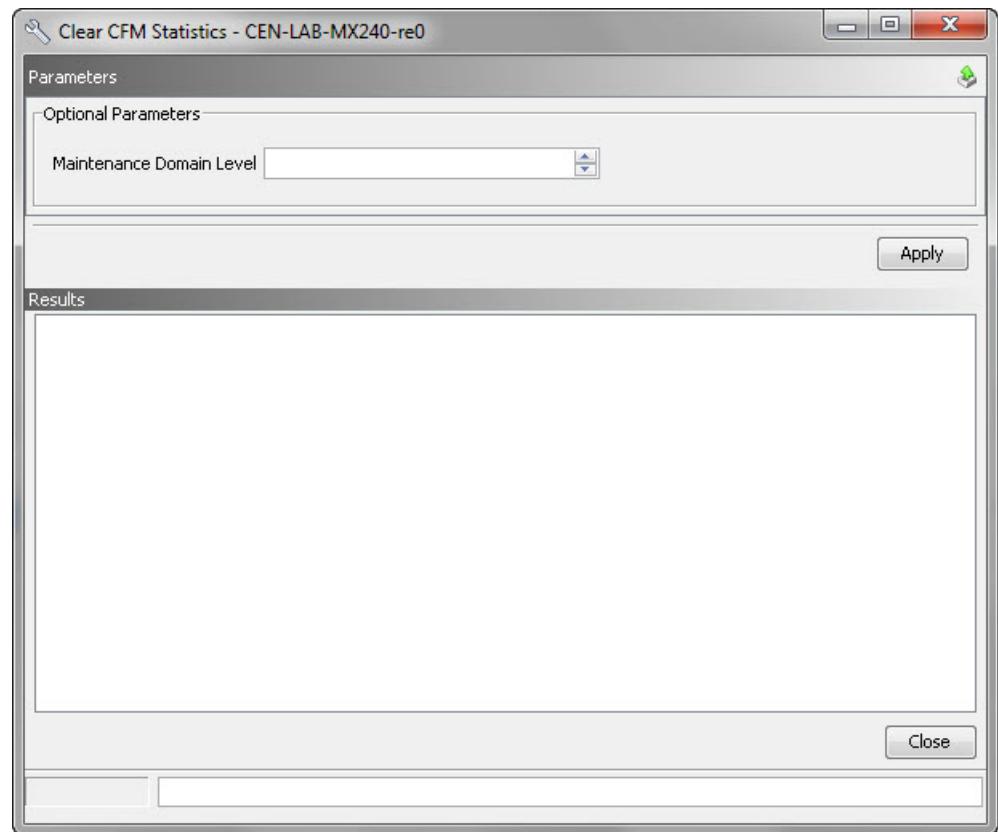
2. If you choose to, define the optional parameters in the fields provided.  
You can move your mouse over the fields for more information and valid values.
3. Click **Apply**.  
The information is displayed in the Results section.
4. If you want to save the configuration information, you can “Save the visible table data to a file” on page 24.
5. When you are finished viewing the information, click **Close** to close the window.

### Clear CFM Statistics

1. Do one of the following:
  - To clear CFM statistics at the NE level, in the Network Elements table or the Topology view, right-click the NE and choose **Maintenance** → **Clear** → **Clear CFM Statistics**.
  - To clear CFM statistics at the interface level, in the Network Element View window, right-click the interface and choose **Maintenance** → **Clear** → **Clear CFM Statistics**.

The Clear CFM Statistics window opens. The context is either the NE or the interface, depending on how the window was accessed.

For example:

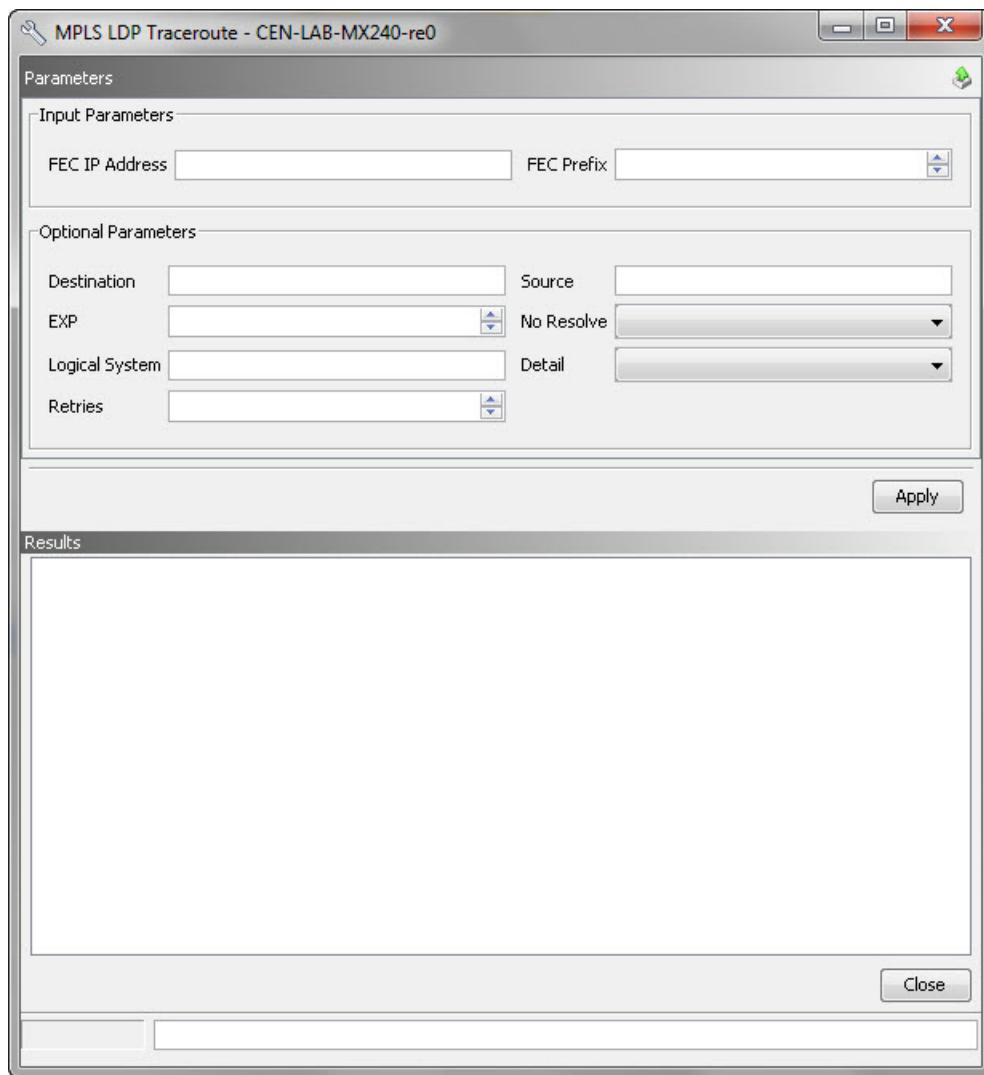


2. If you choose to, define the optional parameters in the fields provided.  
You can move your mouse over the fields for more information and valid values.
3. Click **Apply**.  
The results are displayed in the Results section.
4. If you want to save the configuration information, you can "[Save the visible table data to a file](#)" on page 24.
5. When you are finished viewing the information, click **Close** to close the window.

## 12.4 Perform an MPLS LDP traceroute test

1. In the Network Elements table or the Topology view, right-click the NE and choose **Maintenance** → **Test** → **MPLS LDP Traceroute**.

The MPLS LDP Traceroute window opens for example:



2. Define the input parameters and optional parameters in the fields provided. You can move your mouse over the fields for more information and valid values.
3. Click **Apply**.  
The results are displayed in the Results section.
4. If you want to save the configuration information, you can “Save the visible table data to a file” on page 24.
5. When you are finished viewing the information, click **Close** to close the window.

# 13 Managing SONET cross-connects

The SONET Cross-Connect Manager allows operators to view, create, modify, and delete SONET cross-connects for an NE. It is primarily used to browse and fix individual cross-connects. To create subnetwork cross-connects, use the SONET Domain Controller (SDC). See the SDC documentation for details.

This section contains the following information and procedures for managing cross-connects:

- “View existing SONET cross-connects” on page 153
- “Create a SONET cross-connect” on page 159
- “Delete a cross-connect” on page 163
- “Change the name of a cross-connect” on page 163



Note: If while using the NOC you do not see menu items, tabs or buttons that are described in this documentation, it is because the Network Integrity administrator has not assigned the permission to your user account, or the feature has not been installed.

## 13.1 View existing SONET cross-connects

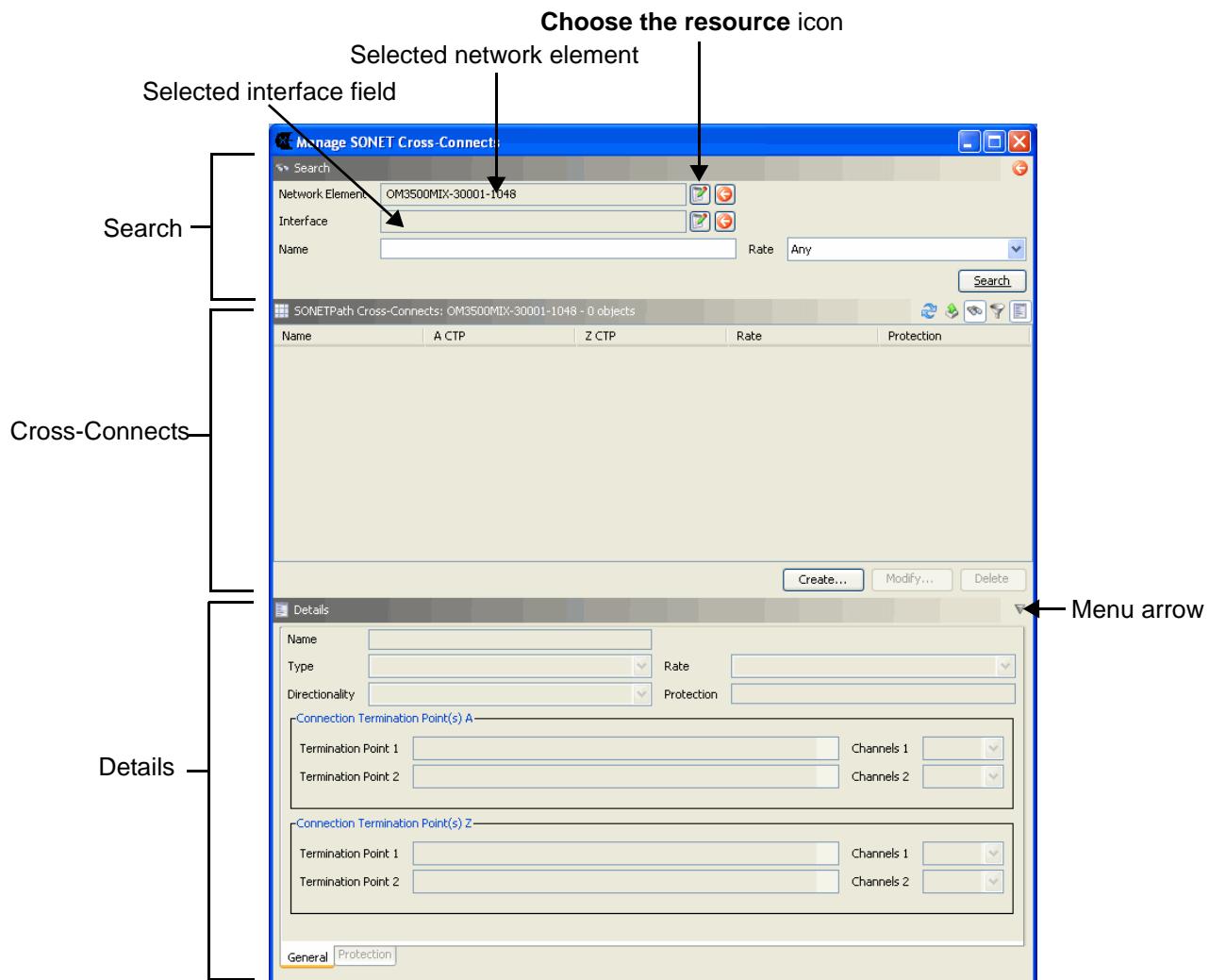
Use this procedure to open the Manage SONET Cross-Connects window and list the existing SONET cross-connects for an NE or for a specific interface on the NE. Cross-connect data is obtained using the Retrieve Service Resources option of a data mining job, which is performed during the Retrieve Resources step. Data mining is described in the Network Integrity Framework Configuration Guide.

1. To view cross-connects for an NE, do one of the following:
  - a. In the main window of the NOC, right-click the NE in the Topology view and select **Provisioning > Manage SONET Cross-Connects**.
  - b. In the main window of the NOC, right-click the NE in the Network Elements table and select **Provisioning > Manage SONET Cross-Connects**.
  - c. In the Network Element View window, right-click the NE and select **Provisioning > Manage SONET Cross-Connects** (see “[Viewing shelf level graphics](#)” on page 42 for more information about the Network Element View).

The Manage SONET Cross-Connects window opens. The window has three sections:

- Search — allows you to specify search criteria for a cross-connect
- Cross-Connects — shows the cross-connects that meet the search criteria

- Details — shows the details for one cross-connect. A Protection tab is available if the cross-connect is a UPSR add/drop cross-connect, or has its source or destination on a 1+1 protected line pair or a 2- or 4-fibre BLSR.



Note: The Details section may not be displayed by default. You can click the **Show/hide details panel** button to display it or hide it.



Note: You can also launch the SONET Cross-Connect Manager by selecting **Provisioning > Manage SONET Cross-Connects** from the menu bar. In this case, the SONET Cross-Connect Manager opens with no fields completed and you must define all of your search criteria. See [Step 5. to Step 9.](#)



Note: You can also launch the SONET Cross-Connect Manager by right-clicking an interface in the Network Element View window and choosing **Provisioning > Manage SONET Cross-Connects** (see [“View shelf, circuit pack, port, and](#)

[interface details](#) on page 48 for how to display interfaces). In this case, the SONET Cross-Connect Manager opens with the Network Element and Interface fields completed. Clicking Search will display all cross-connects matching those search criteria.

2. If you want to view all SONET cross-connects for the NE, click **Search**.

You can also narrow your search, for example, to show only cross-connects with a specific rate. See [Step 5.](#) to [Step 9.](#)

The window updates to display the cross-connects on the NE, similar to this example.

Name	A CTP	Z CTP	Rate	Protection
Heliotrope531	LINEOC192 - OC192-12-1 127 LINEOC192 - OC192-11-1 127	LINEOC48 - OC48-5-1 31	STS-1	Partial
Heliotrope331	LINEOC192 - OC192-12-1 31 LINEOC192 - OC192-11-1 31	LINEOC48 - OC48-3-1 31	STS-1	Partial
Heliotrope431	LINEOC192 - OC192-11-1 79 LINEOC192 - OC192-12-1 79	LINEOC48 - OC48-4-1 31	STS-1	Partial
Heliotrope631	LINEOC192 - OC192-11-1 175 LINEOC192 - OC192-12-1 175	LINEOC48 - OC48-6-1 31	STS-1	Partial

The list of cross-connects provides the following information by default:

- **Name:** the name of the cross-connect
- **A CTP:** the connection termination point (CTP) at the A end of the cross connect. For Add/Drop A-end CTPs, there are two values in this field, one for each CTP.
- **Z CTP:** the connection termination point (CTP) at the Z end of the cross connect. For Add/Drop Z-end CTPs, there are two values in this field, one for each CTP
- **Rate:** the data rate of the cross-connect
- **Protection:** one of the following:

**Unprotected** — Neither side of the cross-connect is protected.

**Partial** — Only side of the cross-connect is protected.

**Full** — Both sides of the cross-connect are protected.

**Preemptible** — The cross-connect uses extra traffic TTPs in a BLSR protected fiber.

You can add or remove columns (see “[Add or remove columns in a table](#)” on page 22).

3. To view details about a cross-connect, do the following:
  - a. Ensure that the Details panel is displayed.

If it is not displayed, click the **Show/Hide Details Panel** button to display it.



- In the cross-connects table, click the cross-connect.

The Details panel shows the detailed information about the cross-connect, similar to the following example:

**Manage SONET Cross-Connects**

SONETPath Cross-Connects: OM3500MIX-30001-1048 - 1 objects

Name	A CTP	Z CTP	Rate	Protection
Cerulean	OC48-11-1 Port 1 SONETLine 1	OC12-5-1 Port 1 SONETLine 1	STS-1	Full

**Details**

**General** **Protection**

**Name:** Cerulean  
**Type:** Simple  
**Directionality:** Bidirectional  
**Termination Point(s) A:**

- Termination Point 1: OC48-11-1 Port 1 SONETLine 1
- Termination Point 2: (empty)
- Channels 1: 5
- Channels 2: (empty)

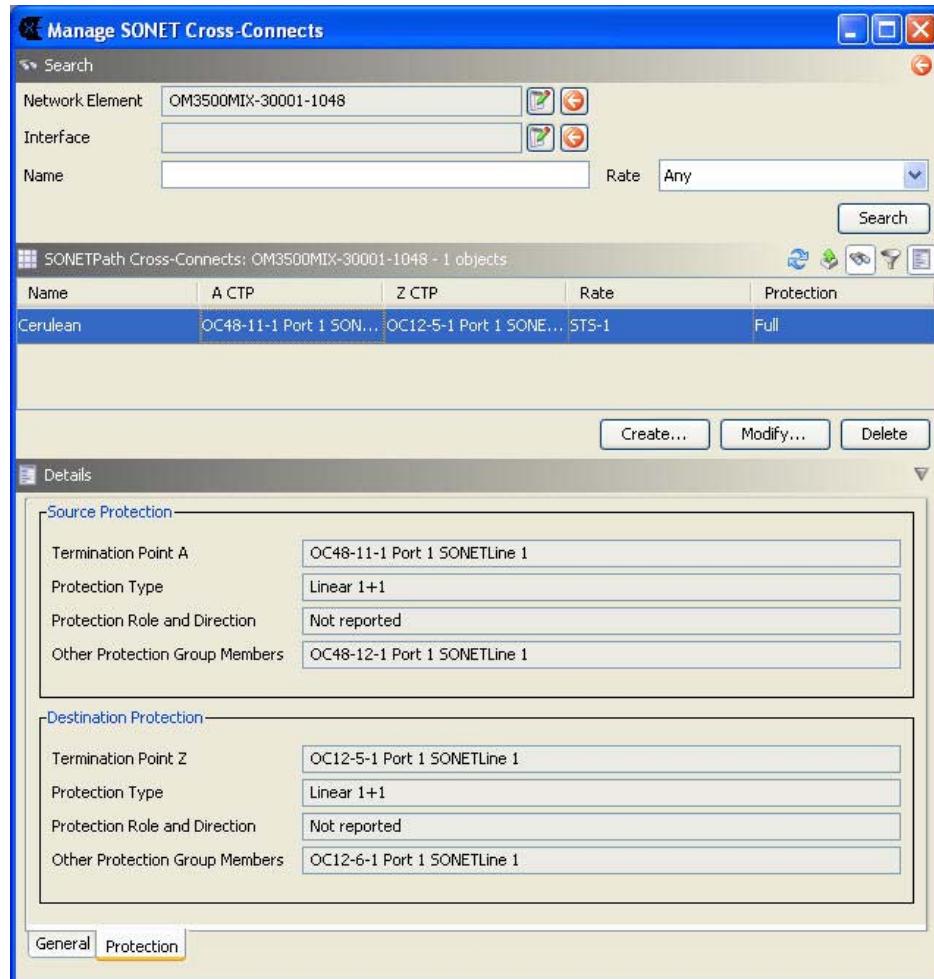
**Termination Point(s) Z:**

- Termination Point 1: OC12-5-1 Port 1 SONETLine 1
- Termination Point 2: (empty)
- Channels 1: 1
- Channels 2: (empty)

You can view cross-connect details in a separate window or view the cross-connect attributes from the network. To do either, right-click the cross-connect in the list or click the menu arrow in the Details panel and choose Inventory > Details or Inventory > View Attributes from Network.

- If the cross-connect is a UPSR add/drop cross-connect, or has its source or destination on a 1+1 protected line pair or a 2- or 4-fibre BLSR, you can click the

**Protection** tab to view protection details for both the source and the destination ends of a cross-connect, similar to the following example:



Protection information includes:

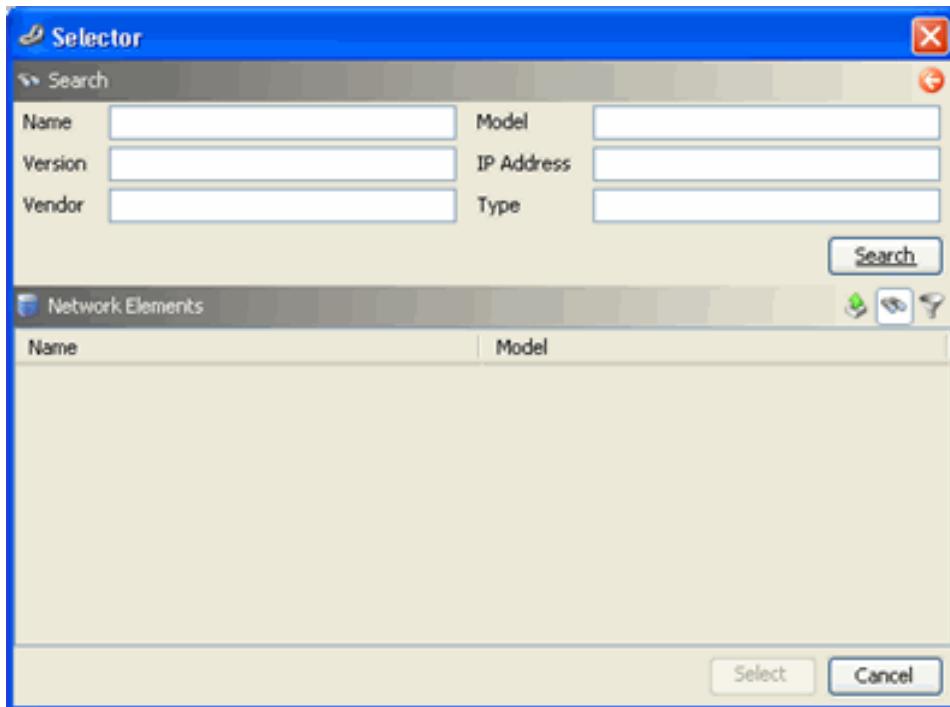
- Protection Type — the type of protection for the cross-connect, for example, Linear 1+1 or UPSR
- Protection Role and Direction — the member's protection role and, where applicable (UPSR and BLSR), the ring direction, for example, "Protecting, West"
- Protection Group Members — other members of the protection group, excluding the one for which details are shown

5. To change the Network Element field, click the **Choose the resource** icon.

The system displays the **Selector** window, which is not populated until a search is performed.

Note: Search is underlined to show that no search has been performed using the currently defined criteria. If the results table is empty and Search is underlined, this indicates that no search has been performed. If the results

table is empty and Search is not underlined, this indicates that the search has returned no results.



- a. If you want to search for all NEs in the system, leave the search fields empty and click **Search**.
- b. If you want to narrow the list, complete any of the search fields and click **Search**.

In the search results, you can do any of the following:

- Hide or show the Search panel by clicking the **Show/Hide Search Panel** button
  - Filter table data. See "[Dynamically filter alarm data](#)" on page 73 for an example of how to do this.
  - "[Sort table data](#)" on page 21
  - "[Add or remove columns in a table](#)" on page 22
  - "[Rearrange the columns in a table](#)" on page 23
  - "[Save the visible table data to a file](#)" on page 24
- c. Choose the NE from the list, then click **Select**.

The NOC places the selected NE name in the Network Element field.

6. To select an interface, click the **Choose the resource** icon beside the **Interface** field.

The system displays the **Selector** window, which is not populated until a search is performed.

- a. If you want to search for all interfaces on the NE, leave the search fields empty and click **Search**.

- b. If you want to narrow the list, complete any of the search fields and click **Search**.

In the search results, you can do any of the following:

- Hide or show the Search panel by clicking the **Show/Hide Search Panel** button
- Filter table data. See “[Dynamically filter alarm data](#)” on page 73 for an example of how to do this.
- “[Sort table data](#)” on page 21
- “[Add or remove columns in a table](#)” on page 22
- “[Rearrange the columns in a table](#)” on page 23
- “[Save the visible table data to a file](#)” on page 24

- c. Choose the interface from the list, then click **Select**.

The NOC places the selected interface in the Interface field.

- 7. To specify a cross-connect name, type all or part of the name in the **Name** field.

If you are using partial names, you must use the wildcard character “\*”. For example, to search for all cross-connects that contain the number 12 anywhere in the name, you would type “\*12\*”.

- 8. To specify a rate, choose the rate from the **Rate** list.

When you click Search, this will update the list of NEs to include only those with cross-connects at the new layer.

- 9. To display a list of cross-connects for the revised selections, click **Search**.

The cross-connects that correspond to your search criteria are displayed. If you click Search and nothing is displayed, it means there are no cross-connects that match your criteria.

You can also perform any of the following procedures:

- Filter table data. See “[Dynamically filter alarm data](#)” on page 73 for an example of how to do this.
- “[Sort table data](#)” on page 21
- “[Add or remove columns in a table](#)” on page 22
- “[Rearrange the columns in a table](#)” on page 23
- “[Save the visible table data to a file](#)” on page 24

## 13.2 Create a SONET cross-connect

Use this procedure to create a SONET cross-connect on an NE. The following types of bidirectional cross-connects are supported:

- simple (one interface on the A-end and one interface on the Z-end)
- add/drop Z-end (two interfaces on the Z-end)
- add/drop A-end (two interfaces on the A-end)

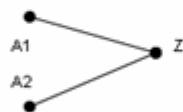
- double add/drop (two interfaces on both the A-end and the Z-end)



Add Drop Z



Add Drop A



Double Add Drop. Each A connected both Zs. Each Z connected to both As.

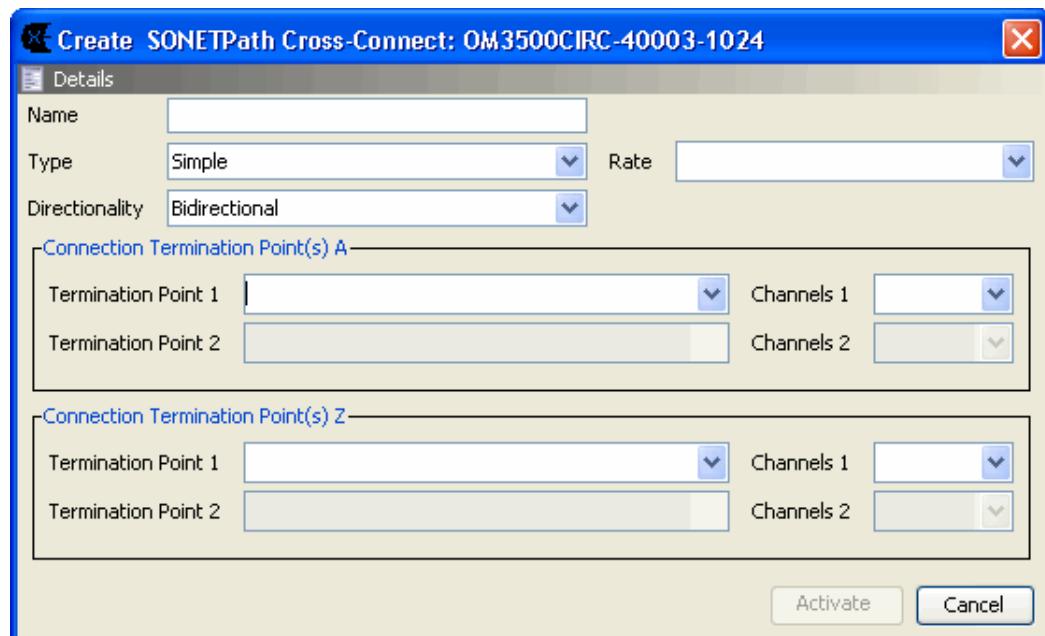


Note: For bidirectional cross-connects, the specification of the A-end and Z-end is arbitrary. For example, if you create an add/drop A-end cross-connect, the network element could change it to an add/drop Z-end cross-connect. This will show up when you view the cross-connect and see that the termination point(s) for the A-end and Z-end have been switched around.

To view details of the cross-connect creation, view the NE Request logs available in the Network Integrity Log Manager. There will be a log for each create and retrieve request. The User logs will show who performed the operation.

1. [View existing SONET cross-connects](#).
2. In the Manage Cross-Connects window, click **Create**.

The Create SONETPath Cross-Connect window opens.



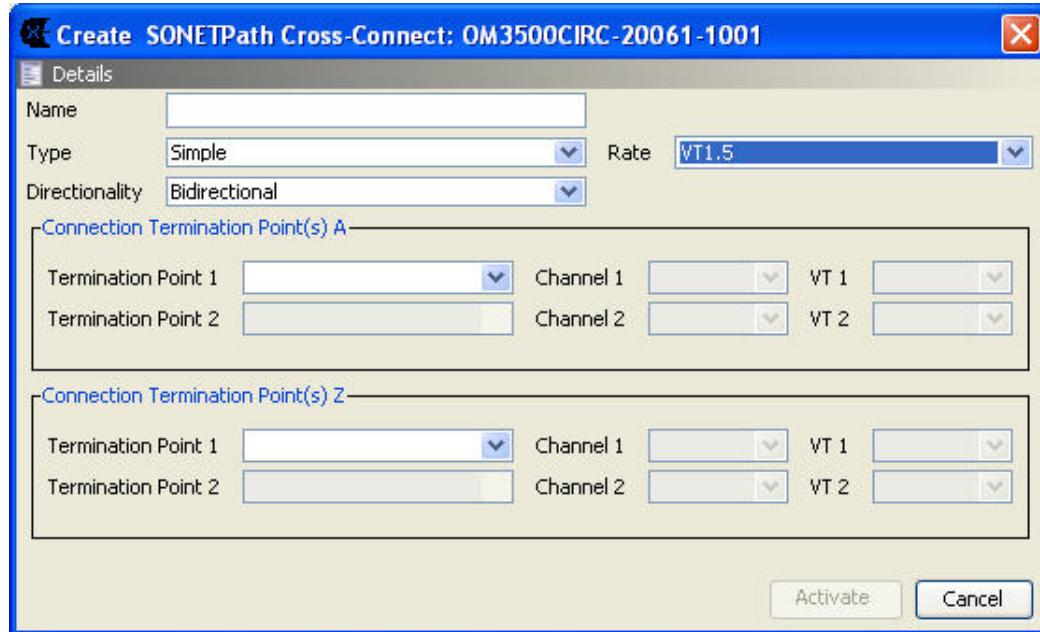
3. Type a name for the cross-connect in the **Name** field.
4. Select a **Type** from the drop-down list: **Simple**, **Add/Drop A-End**, **Add/Drop Z-End**, or **Double Add/Drop**.

Depending on the type of cross-connect you select, a number of the Termination Point/Channel field combinations under Connection Termination Points A and Connection Termination Points Z become available. For example, when Type is set to Simple, only one termination point will be displayed for the A and Z ends.

5. Select a **Rate** from the drop-down lists for each field. The **Directionality** field is always set to "bidirectional" and it is not modifiable.

The rate determines which CTPs you can choose. Only CTPs that support the chosen rate will be available.

If you choose a rate of VT1.5 or 2, the SONETPath Cross-Connect window updates to show additional fields (VT 1 and VT 2) for choosing the virtual tributary on the channel, as shown in the following example:



6. For each available termination point under **Connection Termination Points A** and **Connection Termination Points Z**, perform the following steps:
  - a. Choose Termination Point 1 from the pull-down list.
  - b. Choose Channel 1 from the pull-down list. If the list is empty, it means that there are no channels available.
  - c. If you chose a rate of VT1.5 or VT2, choose a virtual tributary from the VT 1 pull-down list.
  - d. Choose Termination Point 2 from the pull-down list, if applicable.
  - e. Choose Channel 2 from the pull-down list, if applicable. If the list is empty, it means that there are no channels available.
  - f. If you chose a rate of VT1.5 or VT2, choose a virtual tributary from the VT 2 pull-down list, if applicable.



**Note:** You can use an Ethernet termination point as an endpoint if it has a VCG (virtual concatenation group) associated with it. In this case, the valid channels depend on the VCG settings (rate and number of members). If there is no VCG associated with the Ethernet termination point, it can still be chosen as an endpoint for a SONET cross-connect but the valid channels list will be empty.

7. Click **Activate**.

In the Edit Cross-Connect window, under List, the cross-connect that you created is displayed.

8. Perform [Step 2](#). through [Step 7](#). for each cross-connect that you want to create on the NE.

### 13.3 Delete a cross-connect

Use this procedure to delete a cross-connect from an NE.

1. [View existing SONET cross-connects](#).
2. In the list of cross-connects, select the cross-connect that you want to delete, and click **Delete**.  
A message is displayed asking you to verify the deletion.
3. Click **Yes**.  
The cross-connect is removed from the list.



**Note:** You can also right-click the cross-connect and choose **Provisioning > Delete** or click the menu arrow in the Details section and choose **Provisioning > Delete**.

### 13.4 Change the name of a cross-connect

Use this procedure to change the name of a cross-connect on NEs that support cross-connect naming. If you want to change any other attribute of a cross-connect, you must delete it and then create a new one.

If the cross-connect is a VCG member, the name change will also be shown when you [“View VCGs for an NE or group” on page 175](#).

1. [“View existing SONET cross-connects” on page 153](#).
2. In the list of cross-connects, select the cross-connect that you want to delete, and click **Modify**.

The Modify Cross-Connect window opens.

3. Type a new value in the **Name** field.
4. Click **Modify**.

A message is displayed stating that the cross-connect has been modified.

5. Click **OK**.

In the list of cross-connects, the name is modified.



Note: You can also right-click the cross-connect and choose **Provisioning > Modify** or click the menu arrow in the Details section and choose **Provisioning > Modify**.

# 14 Managing links

The Link Manager allows authorized users to view the links between NE endpoints in the NOC, and to create manual topology links between any two NE endpoints visible in the NOC.

Manually created links are managed along with the discovered NE-to-NE links and NE-to-NE links that are derived from interface-to-interface links. The derived links are bundled at the Network Layer by Network Integrity so that many interface-to-interface links at the same Network Layer between two NEs are converted to one NE-to-NE link at that Network Layer.

The link list allows network administrators to see details about all the links between any two NEs. Manually created NE-to-NE topology links are shown in the Topology view when "NE to NE" is selected in the layer selector.

You have the option of launching the Link Manager from a group or network element. If you launch it from a group, you can search for all links in the group. If you launch it from a network element, you can search for links that include that network element.

This chapter contains the following procedures for viewing and managing topological links between NEs using the NOC Link Manager:

- “View links for an NE or group” on page 165
- “Create a manual topology link between two NEs” on page 170
- “View manual topology links in the Topology view” on page 174
- “Delete a manual topology link” on page 174



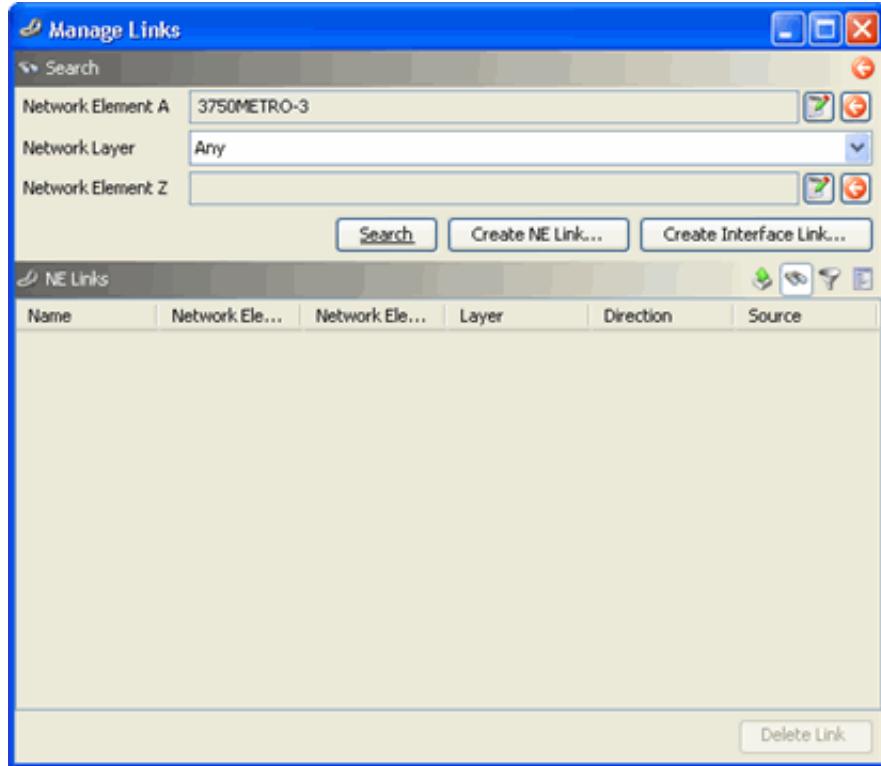
**Note:** If while using the NOC you do not see menu items, tabs or buttons that are described in this documentation, it is because the Network Integrity administrator has not assigned the permission to your user account, or the feature has not been installed.

## 14.1 View links for an NE or group

Use this procedure to launch the Link Manager and view links for an NE or group.

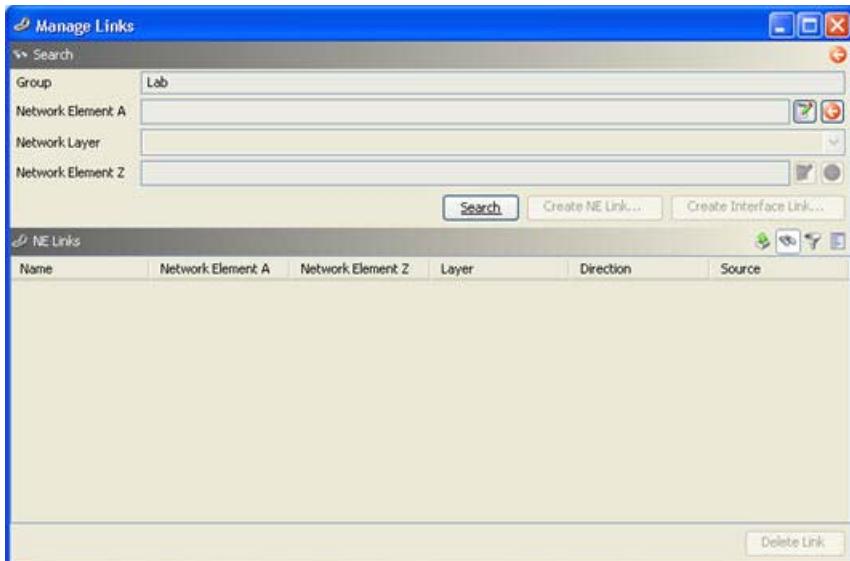
1. Do one of the following:
  - a. If you want to view links for an NE, in the Network Elements table or Topology view, right-click the NE for which to view links and select **Provisioning > Manage Links**.

The Manage Links window opens. The Network Element field contains the NE that you chose, for example:



- b. If you want to view links for a group, in the Groups list or Topology view, right-click the group for which to view links and select **Provisioning > Manage Links**.

The Manage Links window opens. The Group field contains the group that you chose, for example:



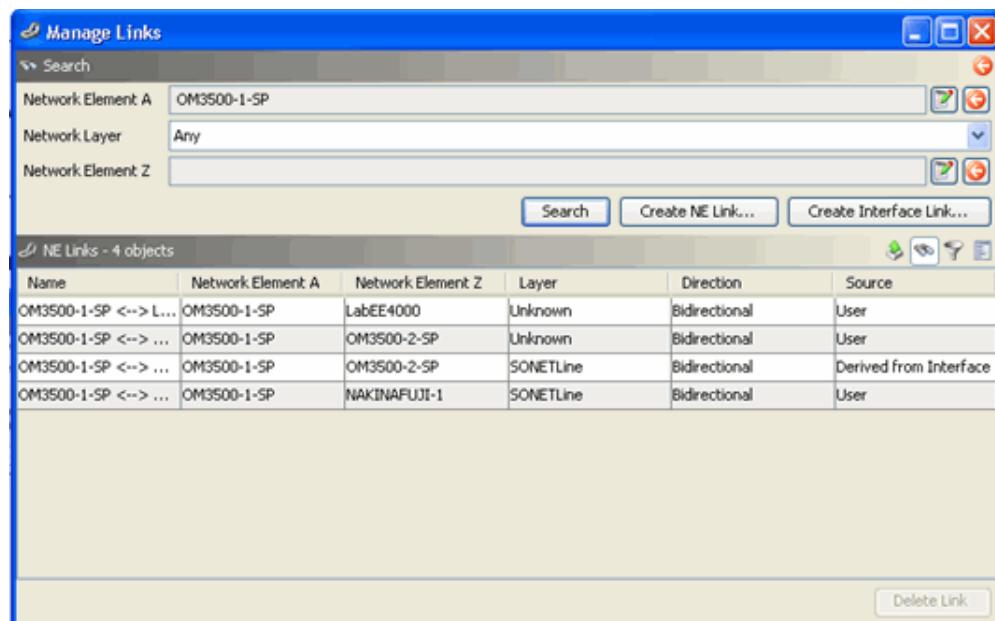
Note: You can also launch the Link Manager by selecting **Provisioning > Manage Links**. In this case, the Link Manager opens with no fields completed and you must define your search criteria. See [Step 4.](#) to [Step 6.](#)

2. If you want to view all links for the NE or group, click **Search**.

You can also narrow your search, for example, to show links only between two NEs or at a specific layer. See [Step 4.](#) to [Step 6.](#)

Note: Search is underlined to show that no search has been performed using the currently defined criteria. If the results table is empty and Search is underlined, this indicates that no search has been performed. If the results table is empty and Search is not underlined, this indicates that the search has returned no results.

The window updates to show the list of links for the NE or group. In the following example, the list of links is for an individual NE.



The list of links provides the following information:

- **Name:** the name of the link
- **Network Element A:** the name of the network element at the A-end of the link
- **Network Element Z:** the name of the network element at the Z-end of the link
- **Layer:** the network layer of the link
- **Direction:** the direction of the interface traffic: Bidirectional, Sink (unidirectional incoming), Source (unidirectional outgoing), or Unknown (Note: all manually created links are indicated as Bidirectional).
- **Source:** the source of the link, either Derived from Interface or User. Derived from Interface indicates that the link was created based on Network Integrity data. User indicates that the link was created by a user.

3. To view details about a link, do the following:

- a. Ensure that the Details panel is displayed.

If it is not displayed, click the **Show/Hide Details Panel** button to display it.



- b. In the **NE Links** table, click the link.

The details are displayed in the Details section at the bottom of the window. The Details section shows information about the NE link that you chose and the interface links associated with it.

Interface links are all of the links between the selected NEs at all layers.

 A screenshot of a software interface titled 'Details'. It contains two main sections: a table for 'NE Links' and a table for 'Interface Links'.
 

Name	OM3500MIX-30011-1040 <--> OM3500MIX-30011-1039	Network Layer	SONETSection
Network Element A	OM3500MIX-30011-1040	Traffic Direction	Bidirectional
Network Element Z	OM3500MIX-30011-1039	Source	Derived from Interface

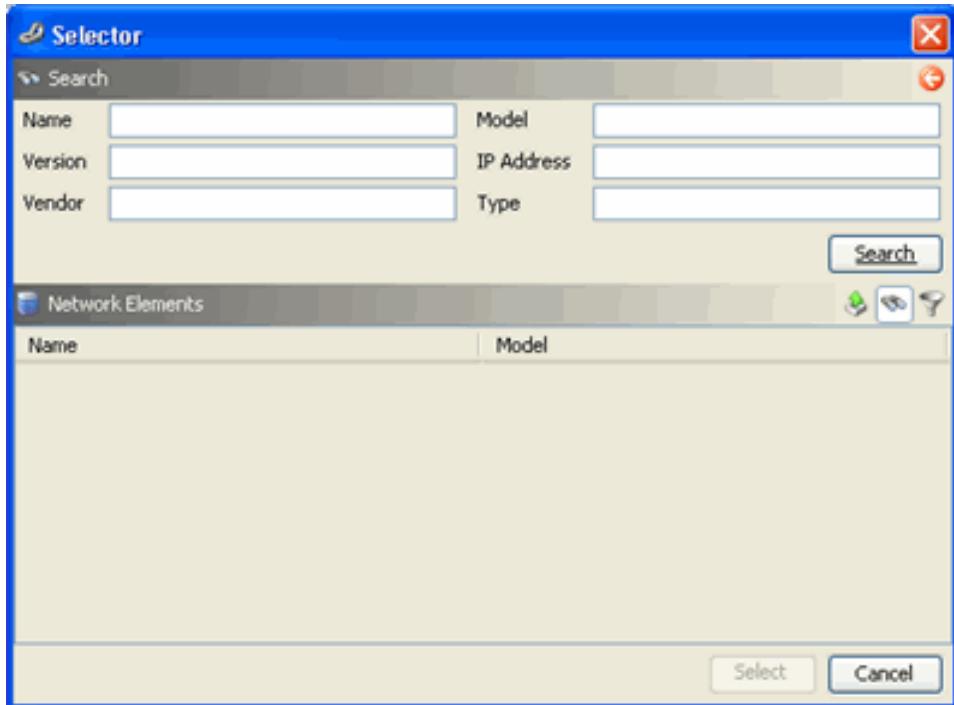
Name	Interface A	Interface Z	Layer	Rate	Direction	Source
SECTIONOC12 - ...	SECTIONOC12 - ...	SECTIONOC12 - ...	SONETSection	OC-12	Bidirectional	Derived from Inte...

4. To change the Network Element A or Network Element Z field, click the **Choose the resource** icon beside the appropriate field.

The system displays the **Selector** window, which is not populated until a search is performed.

Note: Search is underlined to show that no search has been performed using the currently defined criteria. If the results table is empty and Search is underlined, this indicates that no search has been performed. If the results

table is empty and Search is not underlined, this indicates that the search has returned no results.



- If you want to search for all NEs in the system, leave the search fields empty and click **Search**.
- If you want to narrow the list, complete any of the search fields and click **Search**.

In the search results, you can do any of the following:

- Hide or show the Search panel by clicking the **Show/Hide Search Panel** button
- Filter table data. See “[Dynamically filter alarm data](#)” on page 73 for an example of how to do this.
- “[Sort table data](#)” on page 21
- “[Add or remove columns in a table](#)” on page 22
- “[Rearrange the columns in a table](#)” on page 23
- “[Save the visible table data to a file](#)” on page 24
- c. Choose the NE from the list, then click **Select**.

The NOC places the selected NE name in the Network Element field.

5. To change the network layer, choose a new layer from the Network Layer list.

When you click Search, this will update the list of NEs to include only those with links at the new layer.

6. To display a list of links for the revised selection, click **Search**.

The links that correspond to your search criteria are displayed. If you click Search and nothing is displayed, it means there are no links that match your criteria.

You can also perform any of the following procedures:

- Filter table data. See “[Dynamically filter alarm data](#)” on page 73 for an example of how to do this.
- “[Sort table data](#)” on page 21
- “[Add or remove columns in a table](#)” on page 22
- “[Rearrange the columns in a table](#)” on page 23
- “[Save the visible table data to a file](#)” on page 24

## 14.2 Create a manual topology link between two NEs

Use this procedure to create a manual topology link between two NEs at the NE level or at the interface level. You can create links between two NEs that do not have a link, or replace an existing data mined link. Manually created topology links are shown in the Topology view when “NE to NE” or “All Layers” is selected in the layer selector.



**Note:** If you replace a data mined link with a manual link and you want to restore the original link, you must manually delete the link and then mine for data. Data mining is described in the Network Integrity Framework Configuration Guide.



**Note:** In the Link Manager, the buttons for creating links are only available if the Network Element A field is populated. Before you perform this procedure, ensure that you have chosen a Network Element A.

**Table 14–1: Fields in the Create NE Link and Create Interface Link windows**

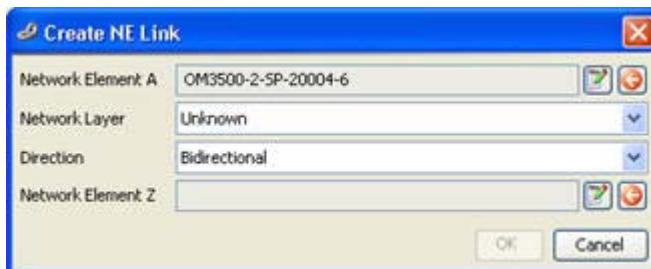
Field	Description
Group	If you searched for links within a group, the Group field identifies the group.
Network Element A	The name of the network element at the A end of the link.
Network Layer	The network layer of the link.  You can create an NE link or an interface link at any network level supported by the NE. The Link Manager will determine the list of available network layers after you choose Network Element A. If you also choose Network Element Z, the Link Manager will further narrow down the network layers list to the layers that are supported by both NEs.  Every NE supports at least the Unknown network layer, so you can use the Unknown layer to create an NE link if no other layers are available. This option is not available for interfaces. If you are creating an interface link and the network layers list becomes empty as a result of selecting a pair of incompatible NEs, you will not be able to create the link.

Field	Description
Direction	The direction of the link, one of: <ul style="list-style-type: none"> <li>Bidirectional — Network Element A and Network Element Z are treated equally as both the source and the destination</li> <li>Source — the link is created from A to Z (Network Element A is the link source, Network Element Z is the destination)</li> <li>Sink — the link is created from Z to A (Network Element A is the link destination, Network Element Z is the source)</li> </ul>
Interface Link A	The name of the interface at the A end of the link. This field is only shown if you are creating an interface link.
Network Element Z	The name of the network element at the Z end of the link.
Interface Link Z	The name of the interface at the Z end of the link. This field is only shown if you are creating an interface link.

1. In the **Manage Links** window, do one of the following:

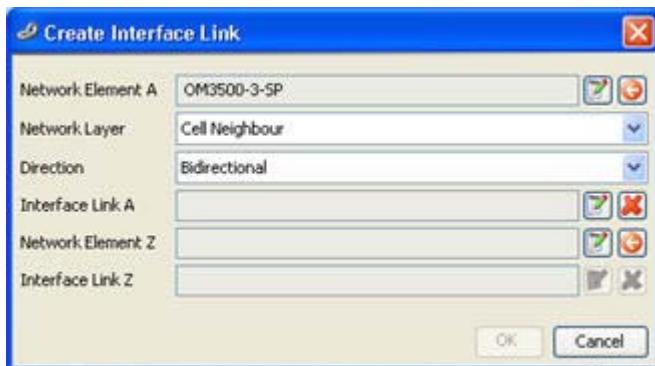
- a. To create an NE-level link, click **Create NE Link**.

The Create NE Link window opens, populated with the Network Element A information from the Link Manager and defaults for Network Layer and Direction.



- b. To create an interface-level link, click **Create Interface Link**.

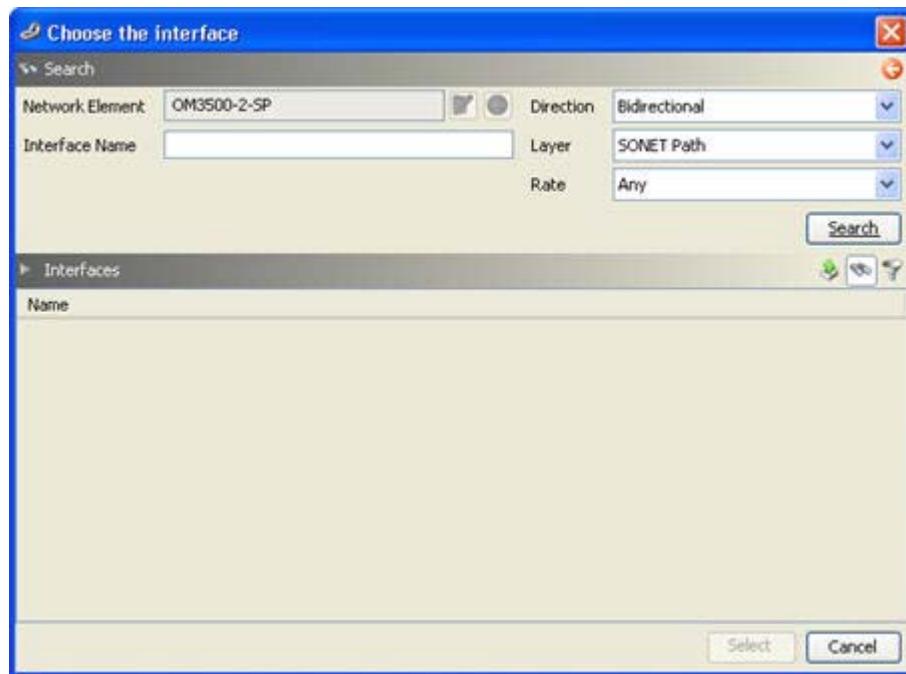
The Create Interface Link window opens, populated with the Network Element A information from the Link Manager and defaults for Network Layer and Direction.



2. From the **Network Layer** list, choose the layer at which to create the link.  
 3. From the **Direction** list, choose the direction of the link.

4. If you are defining an interface link, define Interface Link A by doing the following:
  - a. Click the **Choose the Interface** button next to the **Interface Link A** field.

The Choose the Interface window opens, with the search fields pre-populated with the information from the Create Interface Link window.



- b. Modify the search values or accept the defaults and click **Search**.

You can modify any of the values except Network Element. You can choose a new value from the list for Direction, Layer, or Rate. You can type a value for Interface Name. The wildcard character “\*” is allowed.

In the search results, you can do any of the following:

- Hide or show the Search panel by clicking the **Show/Hide Search Panel** button
- Filter table data. See “[Dynamically filter alarm data](#)” on page 73 for an example of how to do this.
- “[Sort table data](#)” on page 21
- “[Add or remove columns in a table](#)” on page 22
- “[Rearrange the columns in a table](#)” on page 23
- “[Save the visible table data to a file](#)” on page 24

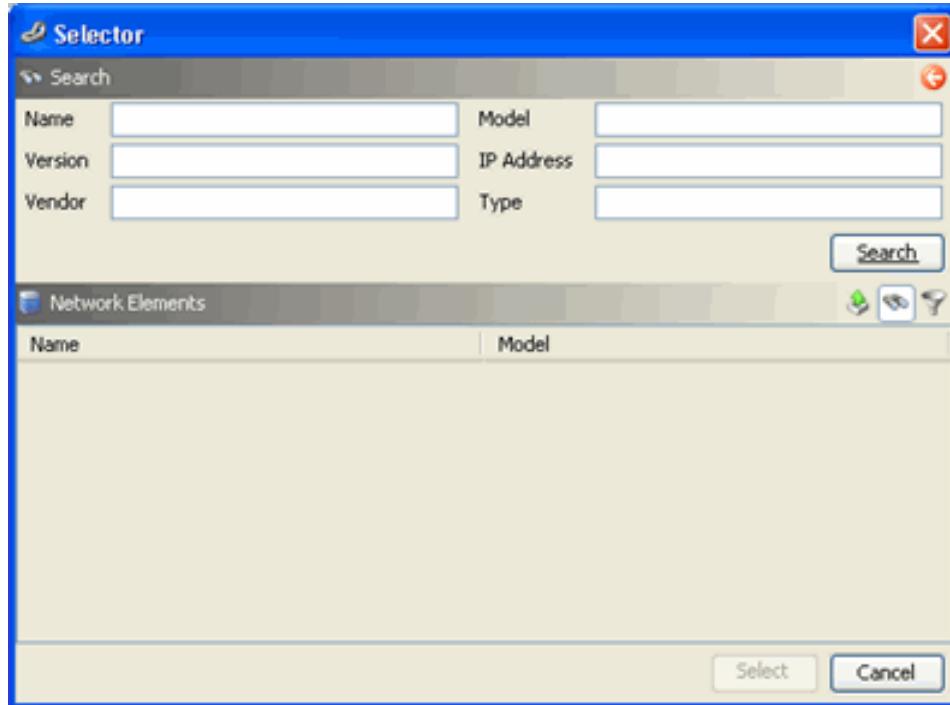
- c. Choose the NE from the list, then click **Select**.

- d. From the list of interfaces, choose the interface and click **Select**.

The NOC places the interface in the Interface Link A field in the Create Interface Link window.

5. Choose the Network Element Z by doing the following (note that if you want to change the Network Element A, you can follow the same steps):
  - a. Click the **Choose the Resource** icon beside the Network Element Z field.

The system displays the **Selector** window, which is not populated until a search is performed.



- b. If you want to search for all NEs in the system, leave the search fields empty and click **Search**.
- c. If you want to narrow the list, complete any of the search fields and click **Search**.

In the search results, you can do any of the following:

- Hide or show the Search panel by clicking the **Show/Hide Search Panel** button
- Filter table data. See “[Dynamically filter alarm data](#)” on page 73 for an example of how to do this.
- “[Sort table data](#)” on page 21
- “[Add or remove columns in a table](#)” on page 22
- “[Rearrange the columns in a table](#)” on page 23
- “[Save the visible table data to a file](#)” on page 24
- d. Choose the NE from the list, then click **Select**.

The NOC places the selected NE name in the Network Element Z field.

6. If you are defining an interface link, define Interface Link Z by repeating [Step 4](#).
7. Click **OK**.

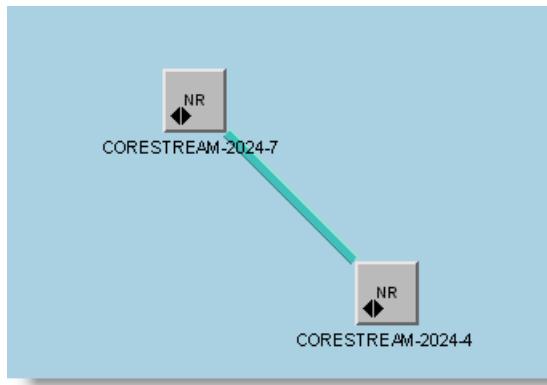
The Link Manager will automatically refresh the NE Links table when an NE link matching the search criteria is created or deleted. Otherwise the NE Links table can be refreshed by clicking the Search button again.

## 14.3 View manual topology links in the Topology view

Use this procedure to view the manual topology links between NEs in the Topology view. Manual topology links are displayed in the NE to NE layer.

1. [“View topology for an NE group” on page 37.](#)
2. From the Layers list, choose NE to NE.

The system displays the manual topology links in the selected group.



Manual topology links are also displayed when you choose “All Layers” from the Layers list.

If no manual links have been created for the group, no links are displayed in the NE to NE layer.

## 14.4 Delete a manual topology link

Use this procedure to delete a manual topology link between two NEs.



Note: The system will not allow you to delete any link other than a manual topology link. The Delete button is only enabled if a manual topology link is selected.

1. [“View links for an NE or group” on page 165.](#)
2. In the list of links, select the link to be deleted.
3. Click **Delete**. (If the Delete button is not enabled, the selected link is not a manual topology link.)
4. In the confirmation dialog box, click **Yes**.  
The selected link is removed from the Network Integrity database.
5. Close the Link Manager window by clicking the **Close** (X) button at the top right corner of the window.

# 15 Managing VCGs

The VCG Manager allows authorized users to view and manage (modify, delete, and add) virtual concatenation groups (VCGs) on network elements (NEs).

This chapter contains the following procedures for viewing and managing VCGs using the VCG Manager:

- “[View VCGs for an NE or group](#)” on page 175
- “[Modify a VCG](#)” on page 179
- “[Delete a VCG](#)” on page 181
- “[Add a VCG](#)” on page 181

VCG members are also displayed in the SONET Cross-Connect Manager. If you add, delete, or modify a VCG member, the changes will also be shown when you “[View existing SONET cross-connects](#)” on page 153. Similarly, if you change the name of a VCG member, the name will also change in the SONET Cross-Connect Manager.



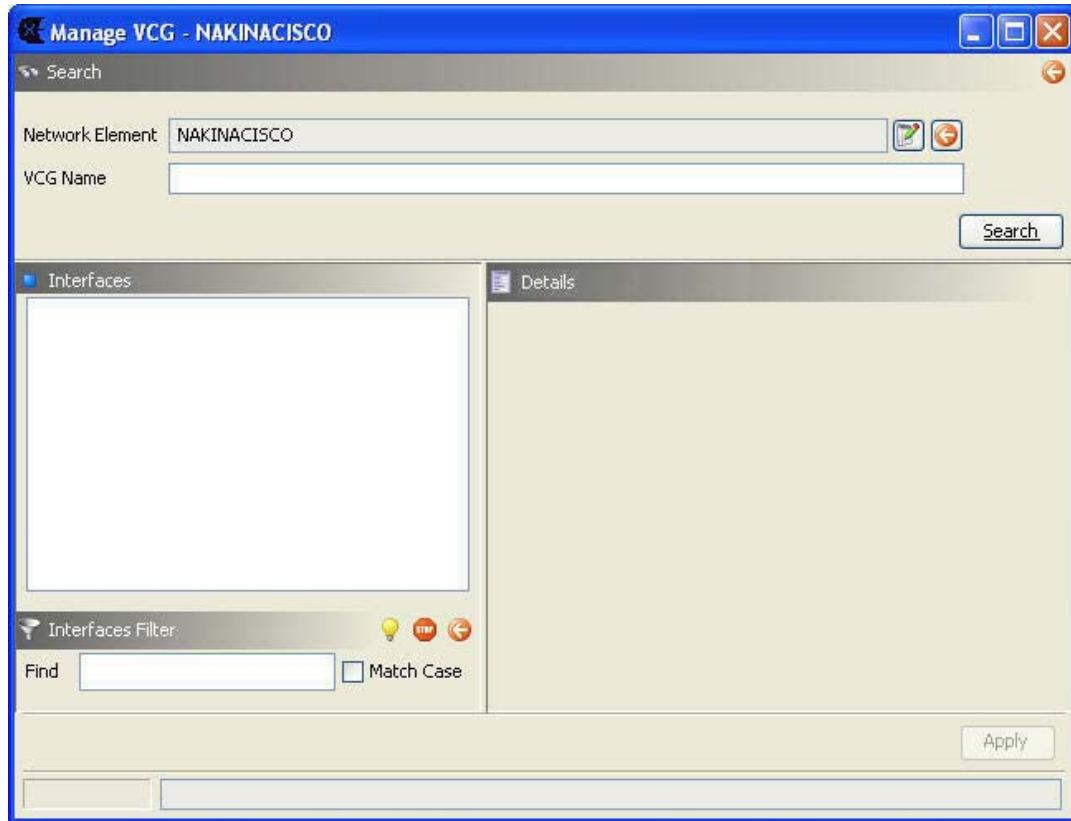
Note: If while using the NOC you do not see menu items, tabs or buttons that are described in this documentation, it is because the Network Integrity administrator has not assigned the permission to your user account, or the feature has not been installed.

## 15.1 View VCGs for an NE or group

Use this procedure to launch the VCG Manager and view VCGs for an NE.

1. In the Network Elements table, Topology view, or Network Element View, right-click the NE for which to view VCGs and select **Provisioning > Manage VCG**.

The VCG Manager window opens. The Network Element field contains the NE that you chose, for example:



Note: You can also launch the VCG Manager by selecting **Provisioning > Manage VCG** from the menu bar. In this case, the VCG Manager opens with no fields completed and you must define your search criteria.

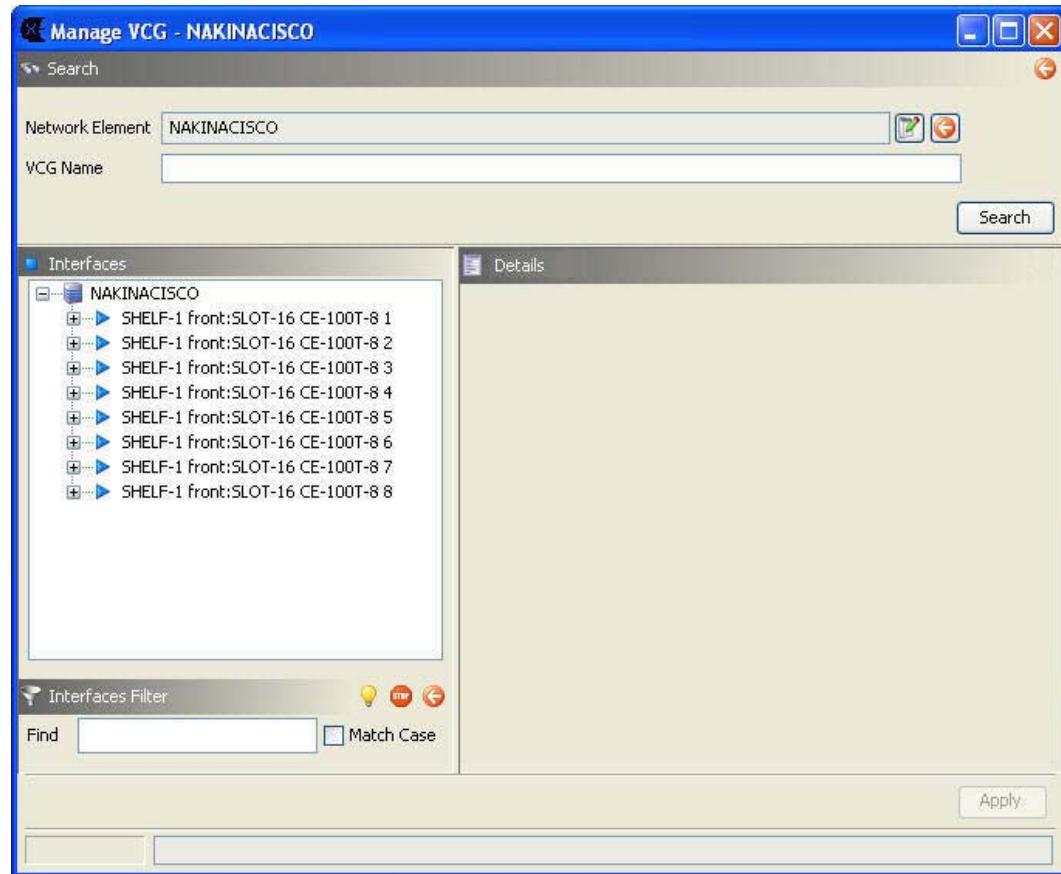
2. Do one of the following:
  - a. If you want to view all VCGs for the NE, click **Search**.
  - b. If you want to search for a specific VCG, type the name or partial name of the VCG in the **VCG Name** field and then click **Search**.

The wildcard character “\*” is allowed.

You can clear the search criteria by clicking the Clear Search Fields button in the top right corner of the window.

Note: Search is underlined to show that no search has been performed using the currently defined criteria. If the results table is empty and Search is underlined, this indicates that no search has been performed. If the results table is empty and Search is not underlined, this indicates that the search has returned no results.

3. The window updates to show the list of Ethernet interfaces that support VCGs on the NE, as shown in the following example:



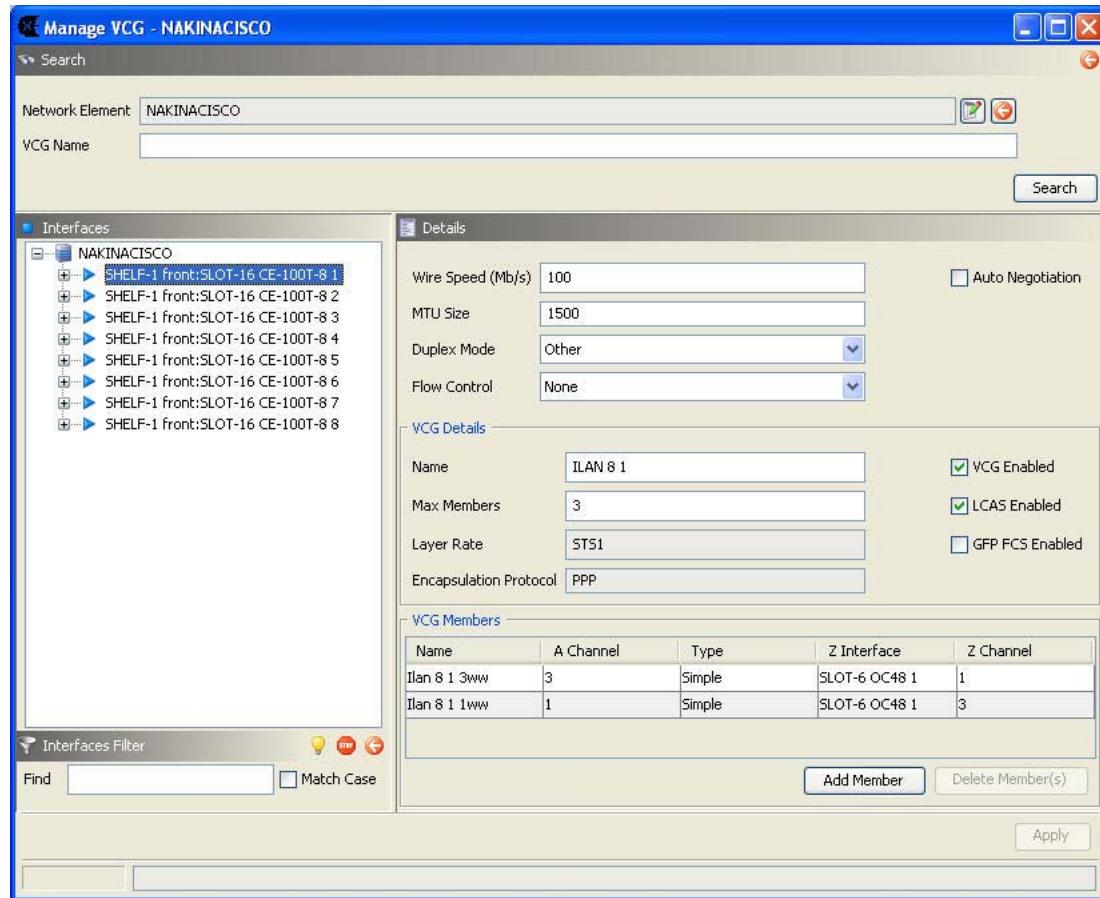
4. If you want to find a specific interface from a long list, you can filter the list using the Interfaces Filter.



As you type in the Find field, the system dynamically displays the matching interfaces. For more information about using the filter, see “[Find network elements](#)” on page 20. Note that highlighting in the VCG Manager is done using bold text, not yellow.

5. To view details about a VCG on an interface, click the interface in the **Interfaces** list.

Details about the VCG are displayed in the VCG Details section of the window. The default values are determined by the adapter.



For each interface, the following information is provided:

- Interface Details:
  - Wire Speed — the wire speed of the interface (i.e., the maximum speed that the hardware can support before software and other overhead costs are added)
  - MTU Size — the size of the largest packet that the interface can transmit (maximum transmission unit)
  - Duplex Mode — the duplex mode that the interface supports (half or full)
  - Flow Control — for full-duplex interfaces, indicates whether flow control is enabled (none, local, full, or passthrough)
  - Auto Negotiation — whether auto negotiation is enabled for the interface
- VCG Details (only displayed if a VCG is assigned to the interface):
  - Name — the name of the VCG
  - Max Members — the maximum number of cross-connects in the Members table. You cannot add more cross-connects than the number shown in this field.
  - Layer Rate — the data rate of the VCG

- Encapsulation Protocol — the technology used for Ethernet frame encapsulation
- VCG Enabled — indicates whether virtual concatenation (VCAT) is enabled. If VCAT is not enabled, there is no traffic being carried on any of the cross-connects in the VCG.
- LCAS Enabled — if enabled, indicates that the VCG supports link capacity adjustment scheme
- GFP FCS Enabled — if enabled, indicates that the VCG supports generic framing procedure frame checking sequence
- VCG Members (only displayed if a VCG is assigned to the interface) — a list of the cross-connects in the VCG

If there is no VCG associated with the interface, no VCG Details or VCG Members are displayed. You can [Add a VCG](#) in this case.

## 15.2 Modify a VCG

In general, for existing VCGs, you can modify the details, VCG name, maximum members, or names of VCG cross-connects (shown in the Members table).

If the VCG has no members, you can also modify the encapsulation protocol.

Changes that you make are shown in bold so that you can confirm that they are correct before you apply them.



**Note:** For both existing and new VCGs, there may be restrictions on which fields you can modify depending on what the adapter and the NE support.



**Note:** For some NEs, you cannot edit the Max Members field. This number is determined by the layer rate. When you select the layer rate, the Max Members field is completed automatically. The layer rate is selectable only if the VCG has no cross-connects.

You can also add or remove cross-connects. You cannot modify existing cross-connects. If you want to modify an existing cross-connect, you must delete it and add a new one.

1. [“View VCGs for an NE or group” on page 175](#)
2. If you want to modify the interface details, do any of the following in the **Details** section:
  - a. In the **Wire Speed** field, type a new value for the maximum speed (Mb/s) that the hardware can support before software and other overhead costs are added.
  - b. In the **MTU Size** field, type a new value for the size of the largest packet, in bytes, that the interface can transmit (maximum transmission unit).
  - c. In the **Duplex Mode** field, choose the duplex mode that the interface supports (half or full).

- d. If the duplex mode is full, in the **Flow Control** field, choose the type of flow control is enabled (none, local, full, or passthrough).
- e. If you want to enable auto negotiation, select the **Auto Negotiation** check box.
3. If you want to change the name of the VCG, type a new name in the **Name** field.
4. If you want modify the encapsulation protocol, choose a new protocol from the **Encapsulation Protocol** list.  
If the VCG already has members, you cannot modify the encapsulation protocol.
5. If you want to change the maximum number of cross-connects, type the new number in the **Max Members** field.  
This is the maximum number of cross-connects in the Members list for the interface. You should choose this value based on how much traffic and how much protection you want on this interface.  
The maximum number you can enter in this field is determined by the layer rate. If you try to enter a number higher than that supported by the layer rate, an error message is displayed and the number does not change.
6. Select the options that apply:
- **VCG Enabled**
  - **LCAS Enabled**
  - **GFP FCS Enabled**
7. If you want to delete a cross-connect, click the cross-connect in the Members table and then click **Delete**.
8. If you want to add a new cross-connect, do the following:
- a. Click **Add Member**.

A new row is added to the Members table, similar to the following:

Members						
Name	A Channel	Type	Z Interface	Z Channel		
lp-222	2	Simple	SLOT-4 OC12 1	8		
lp-333	3	Simple	SLOT-6 OC48 1	7		
	1	Simple				

Add Member      Delete Member(s)

If the layer rate is VT1.5, two extra columns are displayed, A VT and Z VT, similar to the following:

VCG Members						
Name	A Channel	A VT	Type	Z Interface	Z Channel	Z VT
Ilan 8 2 3	1	3	Simple	SLOT-6 OC48 1	2	3-4
Ilan 8 2 5	1	5	Simple	SLOT-6 OC48 1	2	3-3

- b. In the **Name** column, type a name for the new cross-connect.
- c. From the **A Channel** list, choose the A end point of the cross-connect.
- d. From the **Type** list, choose **Simple** or **Add/Drop Z-end**.  
If you choose Add/Drop Z-end, a second row is added so that you can specify two termination points, for example:

Type	Z Interface	Z Channel	
Simple	SLOT-4 OC12 1	8	
Simple	SLOT-6 OC48 1	7	
Add/Drop Z...			

- e. Choose the required **Z Interface** and **Z Channel** termination points for the cross-connect.
  - f. If the layer rate is VT 1.5, choose the A VT and Z VT termination points.
9. Click **Apply**.

The changes are validated and applied to the VCG.

Note: If you make changes to a VCG and do not apply the changes, if you choose another interface or close the window, a warning message will be displayed asking if you want to discard the changes. Click Yes to discard the changes or No to return to the VCG Manager.

## 15.3 Delete a VCG

1. [“View VCGs for an NE or group” on page 175](#)
2. Right-click the interface in the Interfaces list and select **Delete VCG**.
3. Click **Yes** in the confirmation dialog box.

## 15.4 Add a VCG

If there is no VCG associated with an interface, you can add one.

1. [“View VCGs for an NE or group” on page 175](#)
2. Right-click the interface in the **Interfaces** list and click **Add**.  
The Details panel opens with default values.
3. Complete the fields as described in [“Modify a VCG” on page 179](#), with the following exception:

You can also choose a layer rate when creating a VCG, whereas this option is not available when modifying an existing VCG. The layer rate affects the maximum number you can enter in Max Members field. If you try to enter a max members number higher than that supported by the layer rate, an error message is displayed and the max members does not change.

When you choose a layer rate, the Max Members field is automatically set to the maximum number supported by the layer rate.

4. Click **Apply**

Note: After you add a cross-connect to a new VCG, you can no longer modify the layer rate or encapsulation protocol.

# 16 Launching external applications

External applications in the NOC can be available in a number of locations, depending on how your administrator has configured them.

If your administrator has configured the external applications through Session Broker, they may be available from the following locations:

- from the Applications menu  
See “[Use the Applications menu \(global\)](#)” on page 183.
- as applications launched in the context of an NE  
See “[Launch applications in the context of an NE \(Application Launch plugin\)](#)” on page 183

In this case, all login information is handled by Session Broker and you will be logged in automatically.

If your administrator has configured external applications independently of Session Broker, they may be available from the following locations:

- from the NOC application launch pad  
See “[Features of the user interface](#)” on page 11 for more information about the location and content of the NOC application launch pad.
- as custom menu items from an NE  
See “[Use custom NE menu items \(NE Launch-pad plugin\)](#)” on page 184

In this case, login information is not handled by Session Broker and you may need to enter a ID and password. Consult your system administrator for more information.

## 16.1 Use the Applications menu (global)

If your administrator has configured global applications, an Applications menu will be displayed to the right of the Help menu. The contents of the menu are determined by your administrator.

## 16.2 Launch applications in the context of an NE (Application Launch plugin)

Use this procedure to launch an application or executable for an NE (also known as single sign-on). You can use this procedure, for example, to access an NE’s element management system (EMS).

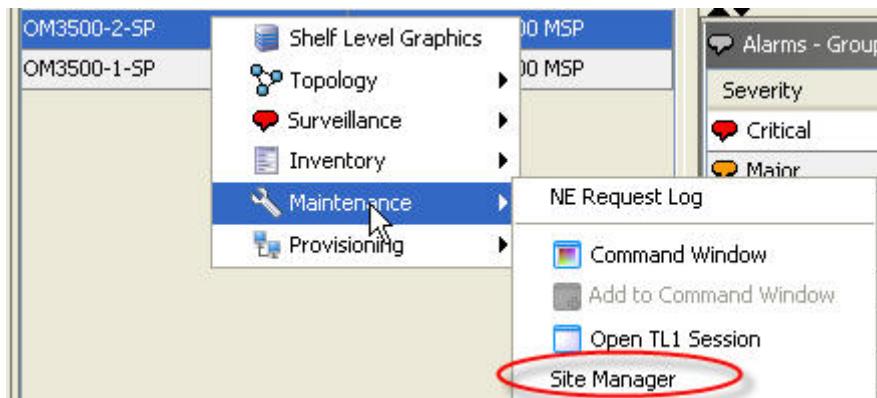
Applications or executables are only available if your administrator has configured access to them using the Network Integrity Framework.



Note: You must log in to the NOC with a valid Network Integrity user ID and password with the correct roles and permissions assigned.

1. In the Network Elements table or Topology view, click on the NE for which you want to launch an application.
2. Right-click and select **Maintenance > <application or executable>**, where <application or executable> is the command defined by your system administrator.

In the following example, the application is named “Site Manager”:



**Note:** The actual command names that are displayed in the pop-up menu will vary according to how the system has been configured. Consult your network administrator if you need clarification on which command launches an application or executable.

The NOC launches the application or executable and logs you in based on credentials configured by your administrator. You may see multiple screens depending on how your administrator has configured the plugin.

Depending on how your administrator configured your system, you may be able to access multiple NEs using the application. In this case, you may need to provide the ID of the NE that you want to access.

## 16.3 Use custom NE menu items (NE Launch-pad plugin)

The NE Launch-pad feature allows administrators to configure the NOC with customized right-click menus that allow a user to access and launch scripts, applications or proprietary NE tools. Menu items are displayed in context with the vendor and model of NE selected. The launch-pad can launch any executable application that the NOC has visibility to on the platform where the NOC is running, such as launching a telnet sessions to a specific port on an NE.

If NE launch-pad has been enabled and configured, this chapter shows how to access applications such as launch vendor provisioning utilities.

Before performing the procedures in this chapter, ensure that an administrator has enabled and configured NE launch pad, according to the NOC Installation and Administration Guide.



**Note:** The NE Launch-pad plugin has been superceded by the Application Launch plugin (described in “[Launch applications in the context of an NE \(Application](#)

"Launch plugin)" on page 183) and will be discontinued in an upcoming release. Nakina recommends that you use the Application Launch plugin.



- Note: If while using the NOC you do not see menu items, tabs or buttons that are described in this documentation, it is because the Network Integrity administrator has not assigned the permission to your user account, or the feature has not been installed.
1. In the Network Elements table or Topology view, click on the NE for which you want to launch an application.
  2. Right-click and select **Maintenance > <application or executable>**, where <application or executable> is the command defined by your system administrator. You may need to enter a user ID and password.

# 17 Issuing TL1 commands

---

The TL1 Command and Control plugin allows users to issue TL1 commands to an NE by doing either of the following:

- typing the command directly into the Command field
- selecting the command from a predefined list

This option is only available if your administrator has created a predefined list of TL1 commands. It eliminates the need for users to manually type in complex TL1 commands by providing a menu of commands to choose from.

If your administrator has created a predefined list of TL1 commands, radio buttons are displayed that enable you to choose whether to type the command manually or choose it from the predefined list. If your administrator has not created a predefined list of TL1 commands, no radio buttons are displayed and your only option is to type the command manually.

When enabled, the TL1 Commands tab appears at the bottom of the network view in both the main NOC window and Shelf Level Graphics (Network Element View window). The tab enables users to issue TL1 commands to one or more NEs, circuit packs, or ports. A menu item is available for NEs, NE groups, and circuit packs. The menu item opens a new window for TL1 Commands.



**Note:** If an NE is out of contact (light blue in color), you cannot issue TL1 commands to it.

This section contains the following information and procedures for using the Command and Control plugin:

- “[About the TL1 Command and Control plugin](#)” on page 186
- “[Issue TL1 commands to NEs, circuit packs, or ports](#)” on page 190

## 17.1 About the TL1 Command and Control plugin

Only authorized users with the correct NOC and Command Broker roles and permissions can access commands on the NEs to which they have been granted access. If the “TL1 Commands” tab is not visible at the bottom of the NOC main window or Network Element View window, it means that this plugin has not been enabled. If a menu of TL1 Commands does not appear in the NOC for a selected model of NE or its circuit pack or ports, it means that predefined commands have not been configured for the NE, circuit pack, or port.

The administrator must use the Network Integrity Framework to define the list of valid TL1 commands, assign a Command Broker User Role to the user, and enable the permission to "Access an NE via Command Broker".

If predefined commands are supported, administrators must also create configuration files in the <NOC>/config directory. One configuration file must be created to define which NEs can be selected for TL1 Command and Control, while other configuration

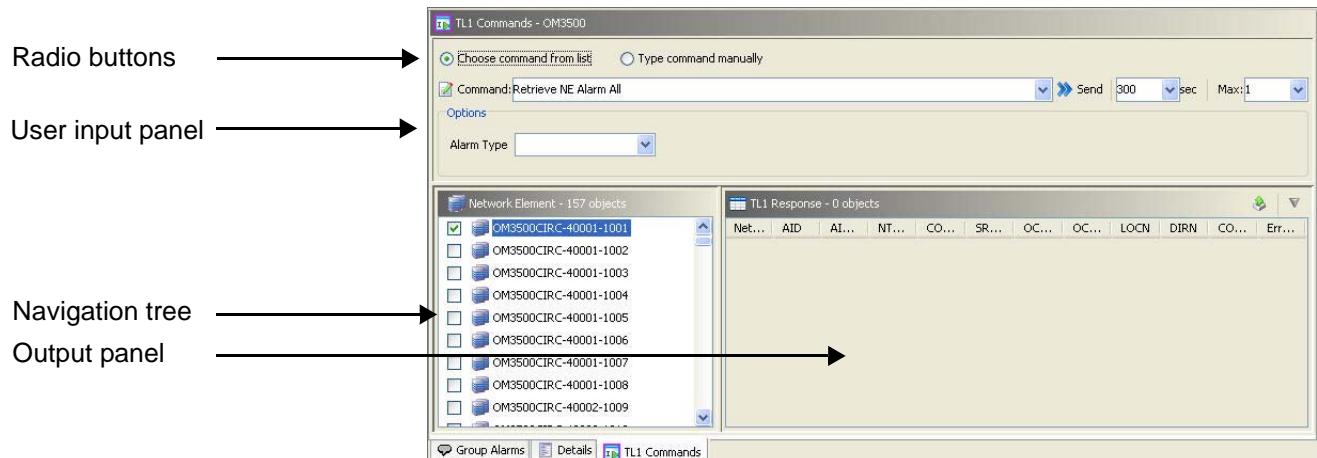
files provide the list of TL1 commands that can be selected by the NOC users. If predefined commands are not supported, this is not necessary.

### 17.1.1 About the TL1 Commands window

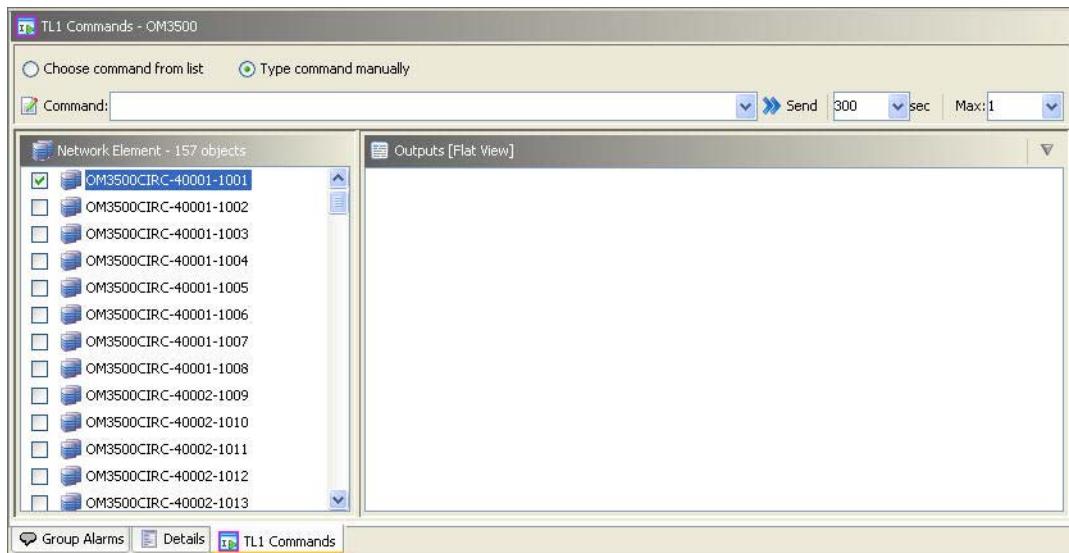
The TL1 Commands window can be displayed in the network view or as a separate window. It consists of three sections:

- radio buttons — enable you to choose whether to type a command manually or choose it from a list  
These buttons are only available if your administrator has configured predefined commands.
- user input panel — allows a user to choose or type commands and define polling settings (see “[About polling](#)” on page 188)  
If predefined commands are available, clicking the arrow will show the available commands. If predefined commands are not available, the list will show only commands that you have typed previously. In this case, you can type the command directly in the Command field.
- navigation tree — allows a user to choose the NEs that the commands apply to
- output panel — shows the results of issuing the command. For predefined commands, this panel is titled TL1 Response. For manually typed commands, this panel is titled Outputs and is not shown in tabular format.

The following example shows the TL1 Commands tab with a predefined command chosen.



The following example shows the same panel for manually typed commands.



## 17.1.2 About polling

When you issue a TL1 command, you can specify polling settings for the command. Polling settings enable you to control:

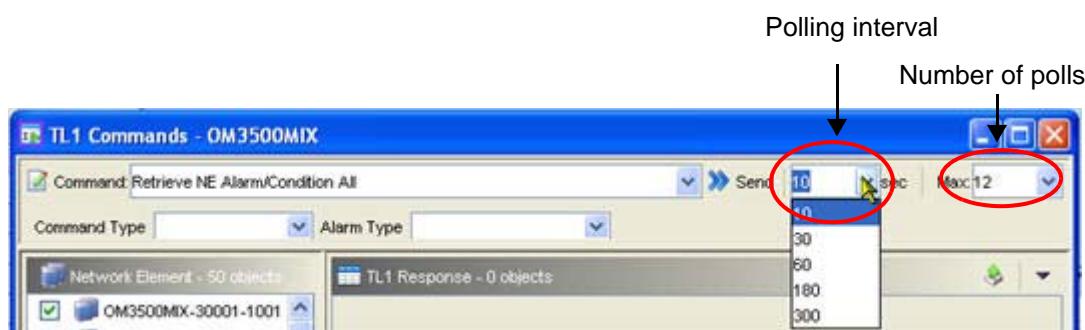
- how often the NOC polls the NEs for updates (the polling interval)

The values in the list (in seconds) are 10, 30, 60, 120, and 300, but you can manually enter any value between 10 and 300.

- how many times the NOC will poll the NEs

The default is 1, but you can enter a value between 1 and 500.

In the following example, the NOC will poll the NEs 12 times with 10 seconds between polls.



**Note:** You cannot change the radio button setting while polling is occurring. The radio buttons are disabled until polling is complete.

### 17.1.3 About command responses

Command responses for predefined commands are displayed, by default, in tabular format, according to the definition provided by the system administrator in the configuration XML file. You also have the option of displaying these in raw TL1 view.

The tabular format appears similar to the following example:

The screenshot shows two windows side-by-side. On the left is a tree view titled 'Network Element - 50 objects' containing several entries for 'OM3500MX-30001-10'. On the right is a table titled 'TL1 Response - 4 objects' with columns: Netwo..., AID, AIPTY..., NTFC..., COND..., SRVEFF, OCRD..., OCRTM, LOCN, DIRN, COND..., Error... . The table contains four rows of data corresponding to the selected network elements.

Netwo...	AID	AIPTY...	NTFC...	COND...	SRVEFF	OCRD...	OCRTM	LOCN	DIRN	COND...	Error...
CM35...	SHELF	COM	MN	FA	NSA	01-01	00-01-	NEND	NA	YPow...	
CM35...	INP	EOPt	MN	INT	NSA	01-01	00-01-	NEND	NA	YRemo...	
CM35...	DS3-7-1	T3	MJ	LOS	SA	01-01	00-03-	NEND	RCV	YDS3...	
CM35...	OC12...	OC12	MN	INC	NSA	01-01	00-33-	NEND	RCV	YSDC...	

In some cases, the responses from the NEs may not match the responses expected by the NOC and defined in the configuration XML file. If this occurs, the NOC handles it as follows:

- If different lines of a response have different numbers of blocks, then extra blocks are discarded.
- If the same block on different lines has a different number of parameters, then extra parameters are discarded.
- If the configuration XML file specifies a block and parameter that does not exist in the response line, then it will be empty in the table.
- If the configuration XML files does not specify a block and parameter that does exist in the response line, then that block/parameter will be discarded.

Command responses for manually typed commands are displayed in raw TL1 view only. For example:

The screenshot shows a window titled 'Outputs [Flat View]' containing a list of command responses. The first response is 'FW4500-30004-1001 rtrv-alm-all'. Subsequent lines show various alarm messages, mostly related to 'Loss of Signal' or 'Loss of Frame' events, with timestamps like '10-02-05 15:26:11' and identifiers like '8781 COMPLD'.

```

FW4500-30004-1001 10-02-05 15:26:11
M 8781 COMPLD
"12-1,T3:CR,LOS,SA,05-19,18-51-34,NEND,RCV:\\"Loss of Signal\\"
"12-1,T3:CR,LOF,SA,05-18,16-28-38,NEND,TRMT:\\"Loss of Frame\\"
"12-2,T3:CR,LOF,SA,05-18,16-28-28,NEND,RCV:\\"Loss of Frame\\"
"12-2,T3:CR,LOF,SA,05-18,16-28-28,NEND,TRMT:\\"Loss of Frame\\"
"12-3,T3:CR,LOF,SA,05-18,16-28-28,NEND,RCV:\\"Loss of Frame\\"
"12-3,T3:CR,LOF,SA,05-18,16-28-49,NEND,TRMT:\\"Loss of Frame\\"
"12-4,T3:CR,LOF,SA,05-18,16-28-28,NEND,RCV:\\"Loss of Frame\\"
"12-4,T3:CR,LOF,SA,05-18,16-28-28,NEND,TRMT:\\"Loss of Frame\\"
"12-5,T3:CR,LOF,SA,05-18,16-28-28,NEND,RCV:\\"Loss of Frame\\"
"12-5,T3:CR,LOF,SA,05-18,16-28-58,NEND,TRMT:\\"Loss of Frame\\"
"12-6,T3:CR,LOF,SA,05-18,16-28-28,NEND,RCV:\\"Loss of Frame\\"
"12-6,T3:CR,LOF,SA,05-18,16-28-28,NEND,TRMT:\\"Loss of Frame\\"
"12-7,T3:CR,LOF,SA,05-18,16-28-28,NEND,RCV:\\"Loss of Frame\\"
"12-7,T3:CR,LOF,SA,05-18,16-29-07,NEND,TRMT:\\"Loss of Frame\\"
"12-8,T3:CR,LOF,SA,05-18,16-28-28,NEND,RCV:\\"Loss of Frame\\"
"12-8,T3:CR,LOF,SA,05-18,16-28-28,NEND,TRMT:\\"Loss of Frame\\"
"1-1-4,STS3C:CR,UNEQ-P,SA,04-29,14-24-32,NEND,RCV:\\"Unequippe
"1-1-7,STS3C:CR,UNEQ-P,SA,04-29,14-24-32,NEND,RCV:\\"Unequippe

```

## 17.2 Issue TL1 commands to NEs, circuit packs, or ports

Use this procedure to issue TL1 commands to one or more NEs, circuit packs, or ports.

You can access the TL1 Commands window in a number of different ways. For example, you can right-click an NE or group in the Topology view or Groups list and choose the appropriate menu items, you can click a group in the Groups list or an NE in the Network Elements table and then click the TL1 Commands tab in the network view, or you can access the window through Shelf Level Graphics (Network Element View window). The procedure explains all of these access methods.

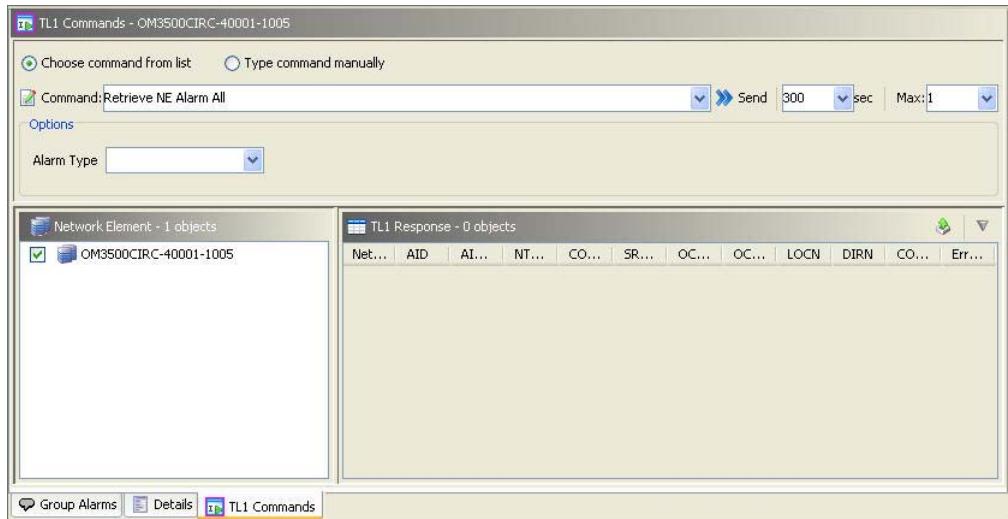
1. Choose the level at which you want to issue TL1 commands.

If you want to	Go to step
issue TL1 commands to a single NE	<a href="#">2.</a>
issue TL1 commands to multiple NEs	<a href="#">3.</a>
issue TL1 commands to a circuit pack, or port	<a href="#">5.</a>

2. To choose a single NE to issue TL1 commands to, do either of the following:

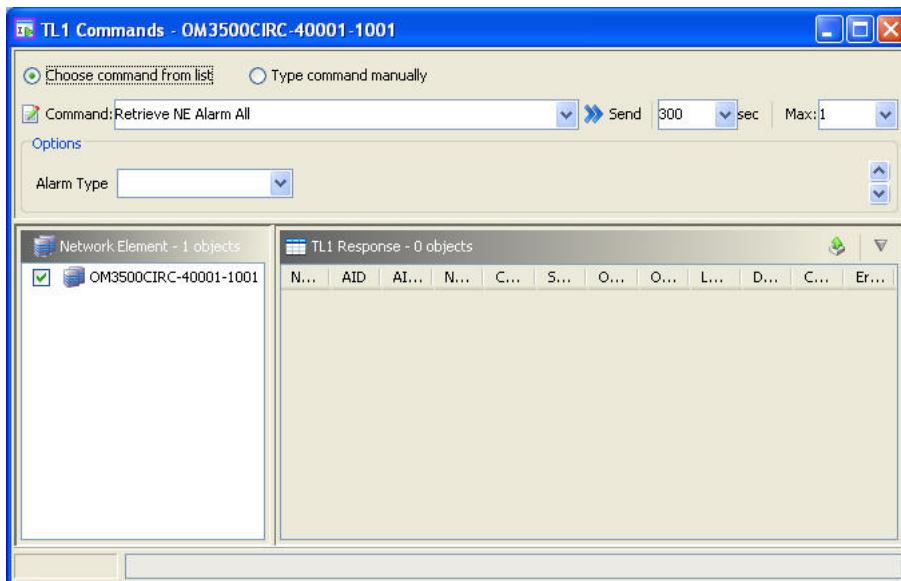
- In the Network Elements table or the Topology view, click the NE that you want to issue commands to and then click the **TL1 Commands** tab in the network view.

The selected NE is displayed in the navigation tree, similar to the following:



- In the Network Elements table or the Topology view, right-click the NE that you want to issue commands to and choose **Maintenance > TL1 Commands**.

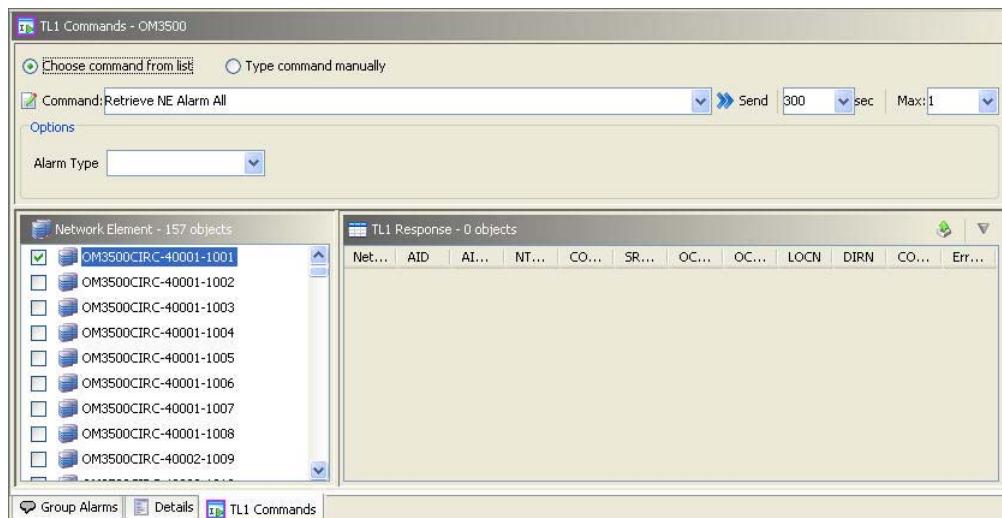
The system displays a new TL1 Commands window with the check box for the NE selected, for example:



**Note:** You can also issue TL1 commands at the NE level from the Network Element View window by clicking the NE and then clicking the TL1 Commands tab or by right-clicking the NE and choosing Maintenance > TL1 Commands. If you choose the second method, a separate TL1 Commands window opens.

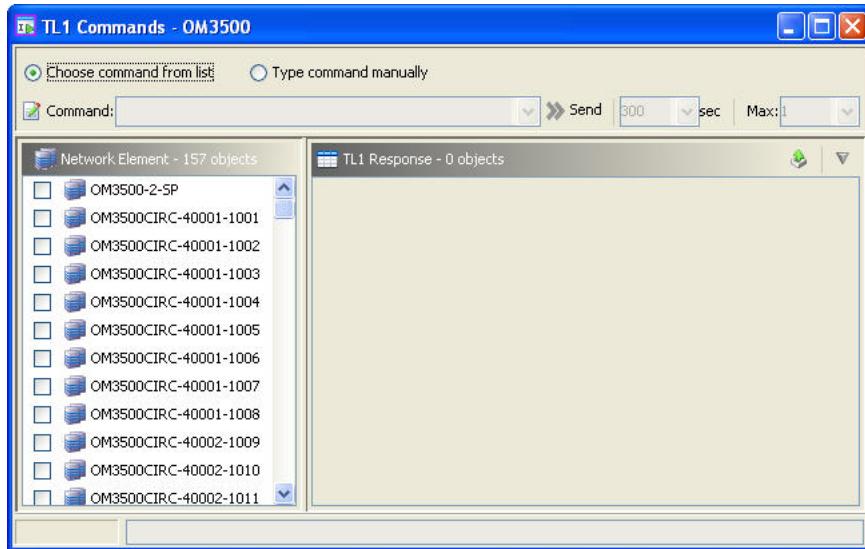
3. To choose multiple NEs to issue TL1 commands to, do either of the following:
  - in the Groups list, click the static or dynamic group that contains the NEs that you want to issue commands to and then in the network view, click the **TL1 Commands** tab.

The NEs in the selected group are displayed in the navigation tree, similar to the following:



- In the Topology view or the Groups list, right-click the static or dynamic NE group that you want to issue commands to and choose **Maintenance > TL1 Commands**.

The system displays a new TL1 Commands window containing the NEs in the group, for example:

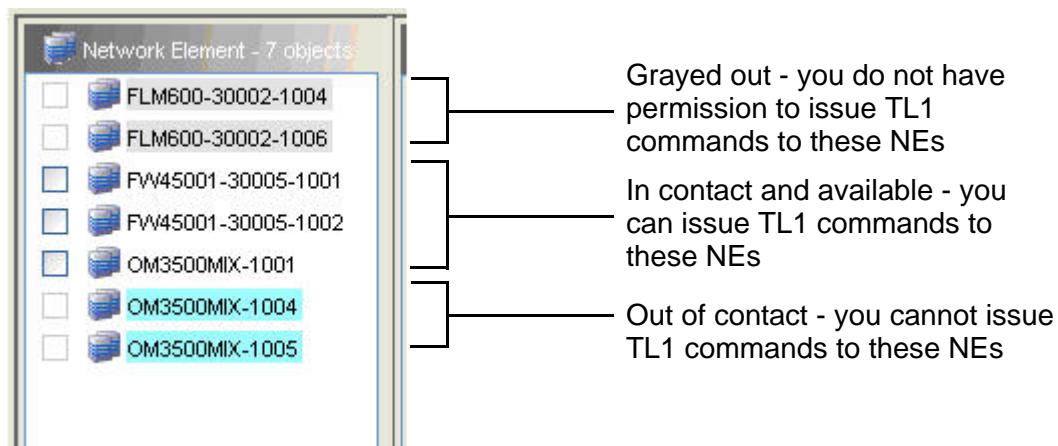


- If you are issuing TL1 commands to multiple NEs, select the check boxes for up to 20 NEs that you want to issue commands to.

When you are selecting check boxes, keep the following in mind:

- If an NE is grayed out, it means that you do not have permission to issue TL1 commands to it.
- If an NE is light blue in color, it is out of contact and you cannot issue TL1 commands to it.
- You can only issue TL1 commands to multiple NEs if they are all the same type.

The following example shows how the NEs are represented.



5. If you are issuing TL1 commands to a circuit pack, or port, do the following:
  - a. ["View shelf, circuit pack, port, and interface details" on page 48.](#)
  - b. Drill down to the level at which you want to issue TL1 commands (shelf, circuit pack or port), and click the **TL1 Commands** tab.

Commands that are available for circuit packs or ports depend on what is defined in the .xml file for the NE type. Only commands that are available for the object that you selected are displayed. For example, at the circuit pack level, only the commands that have been defined for that particular circuit pack type in that NE type are available.

For details, see the NOC Installation and Administration Guide.



**Note:** Note that if you want to open TL1 Commands in a separate window, you can right-click a shelf, circuit pack, or port, and choose Maintenance > TL1 Commands. If you right-clicked a shelf, you must select the check boxes for the circuit cards that you want to issue commands to.

6. If there are radio buttons displayed, choose one of the following options:
  - Choose Command from List
  - Type Command Manually

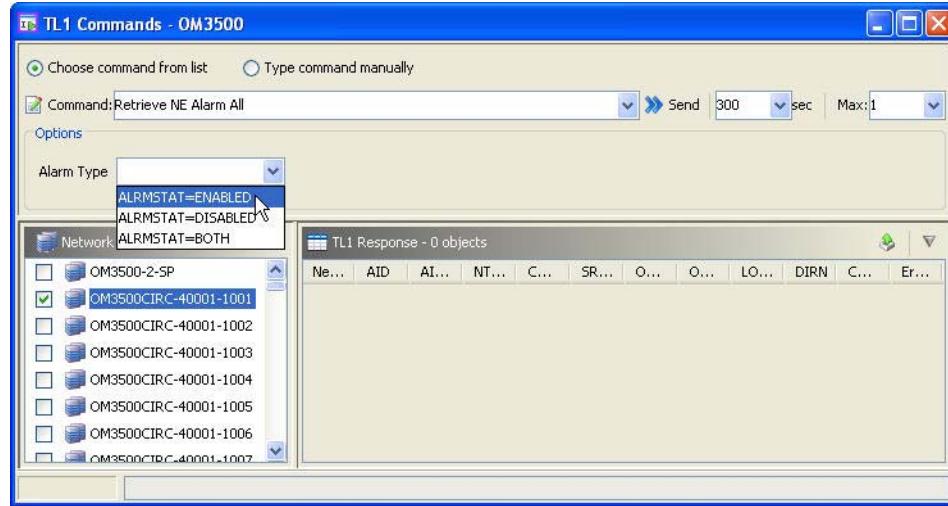
**Note:** If your administrator did not configure predefined commands, no radio buttons are displayed and your only option is to type the command manually.

7. Define the command to issue by doing the following:
  - a. In the **Command** field:

- If you chose "Type Command Manually" or if no radio buttons were displayed, type the TL1 command to issue. If you have issued commands previously, you can click the arrow and choose a command to reissue it.
- If you chose "Choose Command from List", click the arrow, choose the TL1 command to issue and, if there are parameters for the command, choose the parameters (for example, alarm type).

If you do not specify parameters, then all responses matching the command are returned. Otherwise, only the responses that match the parameters are returned. For example, if you do not specify an alarm type, all alarms are returned.

The number of parameters depends on how the commands have been configured. In the following example, there is one parameter for the command.



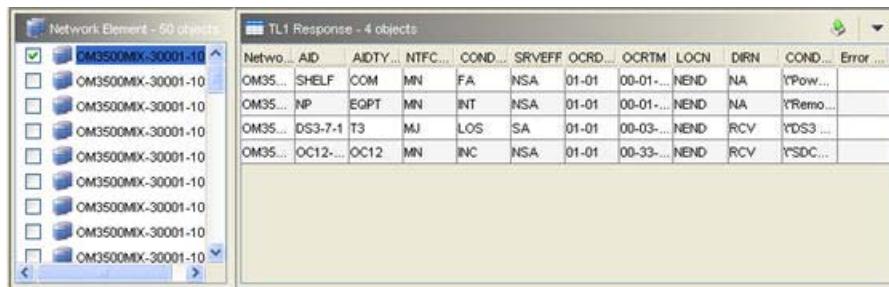
Note: If you have manually typed in commands previously, they are also stored in the pull-down list and you can choose them from this list instead of retyping them. The system stores up to 12 commands.

- Optionally, define the values to use for auto-polling (described in ["About polling" on page 188](#)).
- Click **Send** to issue the command.

Depending on the configuration of the TL1 Command and Control plugin, you may be prompted to confirm the command.

- If prompted, click the appropriate response to confirm the command.

The NOC issues the command to the selected NE or NEs. The command is sent to the NE through the Network Integrity Command Broker application. The system displays the matching responses. For example:



Note: The tabular format shown in the example above is only available for predefined commands. Manually typed commands generate responses similar to the example shown in the TL1 View. For manually typed commands, the response window is titled Outputs.

The command is sent until the auto-polling interval is complete, then the command field is greyed out and the "Send" option changes to "Stop".

You can stop the auto-polling process by clicking **Stop**. Note that this will not stop commands in progress.



8. If you chose a predefined command, to change the view in the TL1 Response table, click the menu arrow and choose an option, as shown in the following example:

Network...	AID	AIDTYPE	NTFCNC...	CONDIT...	SRVEFF	OCDAT	OCRTM	LOCN	DIRN
OM3500...	SHELF	COM	MN	FA	NSA	01-01	00-01-17	NEND	NA
OM3500...	NP	EQPT	MN	INT	NSA	01-01	00-01-45	NEND	NA
OM3500...	DS3-7-1	T3	MJ	LOS	SA	01-01	00-03-03	NEND	RCV
OM3500...	OC12-11	OC12	MN	INC	NSA	01-01	00-33-54	NEND	RCV

- **Group By TID** — groups the responses according to the NE that generated them, for example:

Network Element	AID	AI	NT	C	S	O	O	L	DI	E
Root										
+ OM3500MIX-30001-10										
+ OM3500MIX-30001-10										
+ OM3500MIX-30001-10										
+ OM3500MIX-30001-10										

In this view, you can expand the node to view messages or collapse it. You can also expand or collapse all nodes by right-clicking the root node and choosing Expand All or Collapse All.

- **No Grouping** — displays the responses in the order that they occur (this is the default setting)
- **TL1 View** — shows the raw TL1 commands and responses

Network Element	Time	Message
OM3500MIX-30001-1001	08-05-12 18:43:39	RTRV-ALM-ALL:OM3500MIX-30001-1001::1 OM3500MIX-30001-1001 08-05-12 18:43:39 I COMPLD "SHELF,COM:MN,FA,NSA,01-01,00-01-17,NEND,NA:\"Power Failure - A\"" "NP,EQPT:MN,INT,NSA,01-01,00-01-45,NEND,NA:\"Remote Alarm(s)\"" "DS3-7-1,T3:MJ,LOS,SA,01-01,00-03-03,NEND,RCV:\"DS3 Rx Loss Of Signal\"" "OC12-11,OC12:MN,INC,NSA,01-01,00-33-54,NEND,RCV:\"SDCC Link Failure\""; RTRV-ALM-ALL:OM3500MIX-30001-1001::2 RTRV-ALM-ALL:OM3500MIX-30001-1002::3

In the TL1 Response table, you can also do any of the following:

- “Sort table data” on page 21
- “Add or remove columns in a table” on page 22
- “Rearrange the columns in a table” on page 23
- “Save the visible table data to a file” on page 24
- resize a column by clicking the edge and dragging to increase or decrease the size

- clear all items from the TL1 Response table by clicking the menu arrow and choosing **Clear**.



9. If you typed in a command manually, you can change the view in the TL1 Response section by clicking the menu arrow and choosing an option:

- **Command View** — displays the command at the top of the tree followed by each NE with its associated output
- **NE View** — displays commands by network element
- **Flat View** — displays the command output in the order in which it was executed



10. If you typed in a command manually you can enable display of autonomous messages by clicking the menu arrow and choosing Enable Notification.

A check mark appears beside the Enable Notification command.

An autonomous message is a message that is generated by the NE as a result of a condition on the NE. Selecting Enable Notification means that all autonomous messages issued by the NE(s) will be displayed in the Outputs pane of the command window.

Note: To turn off the display of autonomous messages, choose Enable Notification again. The check mark disappears from the Enable Notification command.

## 18 Viewing outstanding conditions and autonomous messages

The RTRV-COND and RTRV-AO Value Pack plugin provides additional tabs and stand-alone windows for automatically viewing outstanding conditions and autonomous messages. It displays two new tabs at the bottom of the network view:

- Outstanding Conditions — This tab enables users to view outstanding conditions for a single NE (for example, error messages).
- TL1 Autonomous Messages — This tab displays autonomous messages generated by the selected NE or NEs. An autonomous message is a message that is generated by the NE as a result of a condition on the NE, for example, scheduled diagnostic tests.

Each of these tabs executes a single command for the NE or NEs that you select.

This plugin is only available if you have requested it from Nakina.

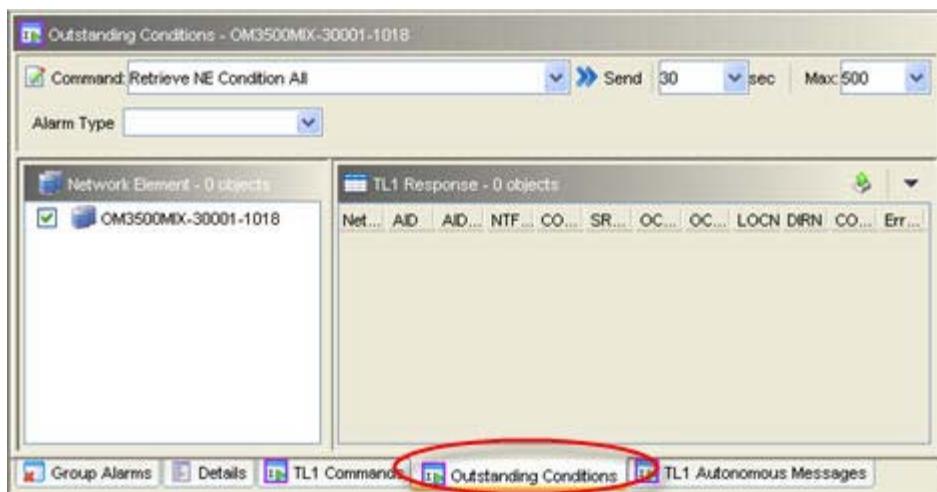
The layout of the window is the same as for TL1 commands. See “[About the TL1 Commands window](#)” on page 187, “[About polling](#)” on page 188, and “[About command responses](#)” on page 189 for details.



**Note:** If an NE is out of contact (light blue in color), you cannot view outstanding conditions or TL1 autonomous messages for it.

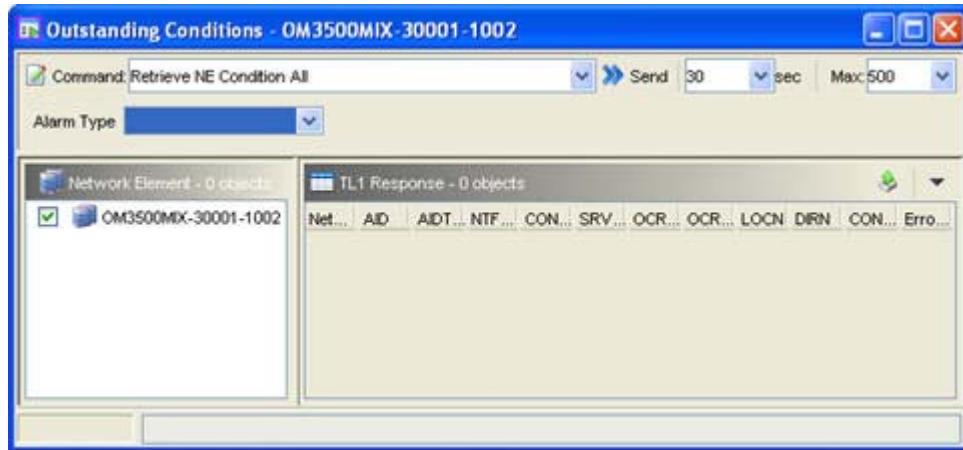
1. To view outstanding conditions or autonomous messages for a single NE, do either of the following:
  - In the Network Elements table or the Topology view, click the NE for which to view outstanding conditions or autonomous messages and then click the **Outstanding Conditions** or **Autonomous Messages** tab in the network view.

The selected NE is displayed in the tree view. The following example shows the Outstanding Conditions tab selected



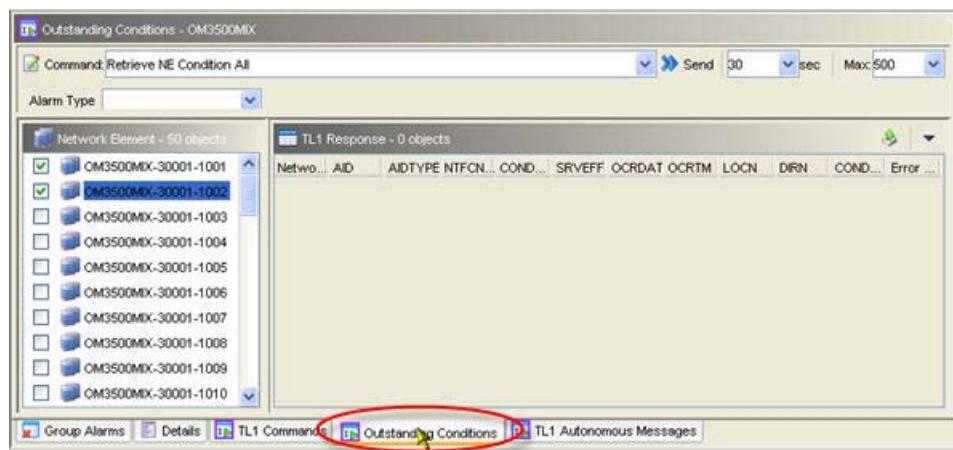
- In the Network Elements table or the Topology view, right-click the NE for which to view outstanding conditions or autonomous message and choose **Maintenance > Outstanding Conditions or Autonomous Messages**.

The system displays a new Outstanding Conditions or Autonomous Messages window with the check box for the NE selected. The following example shows an Outstanding Conditions window.



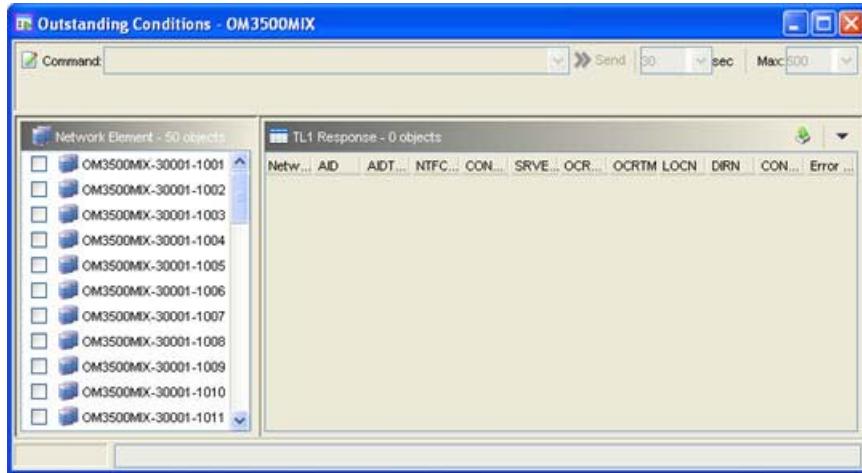
- To view outstanding conditions or autonomous conditions for multiple NEs, do either of the following:
  - in the Groups list, click the group that contains the NEs for which to view outstanding conditions or autonomous messages and then click the **Outstanding Conditions** or **Autonomous Messages** tab in the network view.

The NEs in the selected group are displayed in the navigation tree, similar to the following:



- In the Topology view, right-click the group for which to view outstanding conditions or autonomous messages and choose **Maintenance > Outstanding Conditions or Autonomous Messages**.

The system displays a new Outstanding Conditions or Autonomous Messages window containing the NEs in the group, for example:



- a. If there are parameters for the command, choose the parameters (for example, alarm type).  
If you do not specify parameters, then all responses matching the command are returned. Otherwise, only the responses that match the parameters are returned. For example, if you do not specify an alarm type, all alarms are returned.
- b. Optionally, define polling settings. See “[About polling](#)” on page 188 for details.  
These settings enable you to control how often the NOC polls the NEs for updates and how many times it will do so.
- c. Click **Send** to issue the command.

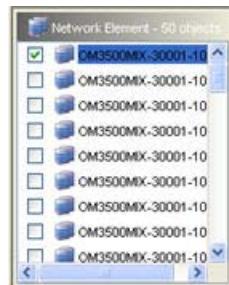
You can stop the process by clicking **Stop**.



Depending on the configuration of the TL1 Command and Control plugin, you may be prompted to confirm the command.

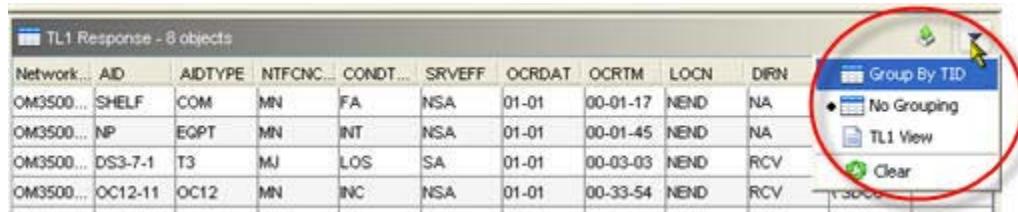
- d. If prompted, click the appropriate response to confirm the command.

The NOC issues the command to the selected NE or NEs. The command is sent to the NE through the Network Integrity Command Broker application. The system displays the matching responses, for example:



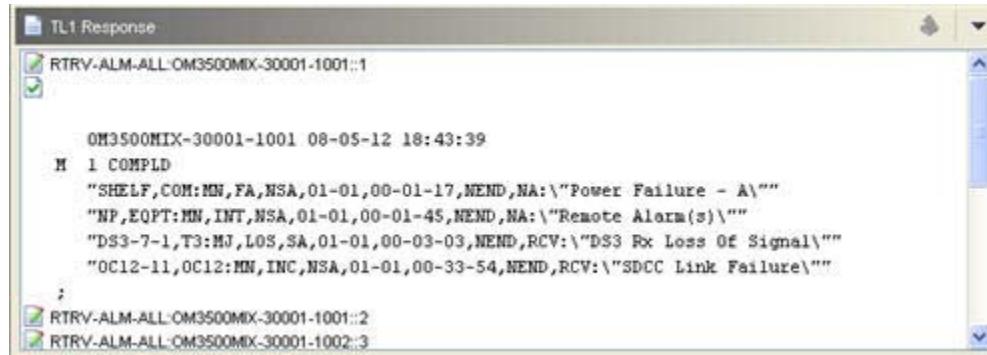
Network...	AID...	AIDTYPE...	NTFCNC...	COND...	SRVEFF...	OCDAT...	OCRTM...	LOCN...	DIRN...	COND...	Error...
OM35...	SHELF	COM	MN	FA	NSA	01-01	00-01-17	NEND	NA	YPow...	
OM35...	NP	EQPT	MN	INT	NSA	01-01	00-01-45	NEND	NA	YRemo...	
OM35...	DS3-7-1	T3	MJ	LOS	SA	01-01	00-03-03	NEND	RCV	YDS3...	
OM35...	OC12...	OC12	MN	INC	NSA	01-01	00-33-54	NEND	RCV	YSDC...	
OM35...	OC12-11	OC12	MN	INC	NSA	01-01	00-33-54	NEND	RCV	YSDC...	
OM35...	OC12-11	OC12	MN	INC	NSA	01-01	00-33-54	NEND	RCV	YSDC...	
OM35...	OC12-11	OC12	MN	INC	NSA	01-01	00-33-54	NEND	RCV	YSDC...	
OM35...	OC12-11	OC12	MN	INC	NSA	01-01	00-33-54	NEND	RCV	YSDC...	
OM35...	OC12-11	OC12	MN	INC	NSA	01-01	00-33-54	NEND	RCV	YSDC...	
OM35...	OC12-11	OC12	MN	INC	NSA	01-01	00-33-54	NEND	RCV	YSDC...	

- To change the view in the TL1 Response table, click the menu arrow and choose an option, as shown in the following example:



Network...	AID...	AIDTYPE...	NTFCNC...	COND...	SRVEFF...	OCDAT...	OCRTM...	LOCN...	DIRN...
OM3500...	SHELF	COM	MN	FA	NSA	01-01	00-01-17	NEND	NA
OM3500...	NP	EQPT	MN	INT	NSA	01-01	00-01-45	NEND	NA
OM3500...	DS3-7-1	T3	MJ	LOS	SA	01-01	00-03-03	NEND	RCV
OM3500...	OC12-11	OC12	MN	INC	NSA	01-01	00-33-54	NEND	RCV
OM3500...	OC12-11	OC12	MN	INC	NSA	01-01	00-33-54	NEND	RCV
OM3500...	OC12-11	OC12	MN	INC	NSA	01-01	00-33-54	NEND	RCV
OM3500...	OC12-11	OC12	MN	INC	NSA	01-01	00-33-54	NEND	RCV
OM3500...	OC12-11	OC12	MN	INC	NSA	01-01	00-33-54	NEND	RCV

- Group By TID** — groups the responses according to the NE that generated them
- No Grouping** — displays the responses in the order that they occur (this is the default setting)
- TL1 View** — shows the raw TL1 commands and responses



```

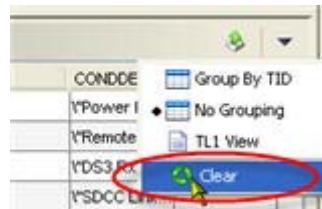
RTRV-ALM-ALL:OM3500MIX-30001-1001::1

OM3500MIX-30001-1001 08-05-12 18:43:39
M 1 COMPL
" SHELF,COM:MN,FA,NSA,01-01,00-01-17,NEND,NA:\\"Power Failure - A\\\""
" NP,EQPT:MN,INT,NSA,01-01,00-01-45,NEND,NA:\\"Remote Alarm(s)\\\""
" DS3-7-1,T3:MJ,LOS,SA,01-01,00-03-03,NEND,RCV:\\"DS3 Rx Loss Of Signal\\\""
" OC12-11,OC12:MN,INC,NSA,01-01,00-33-54,NEND,RCV:\\"SDCC Link Failure\\\""
;
RTRV-ALM-ALL:OM3500MIX-30001-1001::2
RTRV-ALM-ALL:OM3500MIX-30001-1002::3

```

- In the TL1 Response table, you can also do any of the following:
  - ["Sort table data" on page 21](#). Note that you have sorted the table by TID, the sorting will occur within the NE.
  - ["Add or remove columns in a table" on page 22](#)
  - ["Rearrange the columns in a table" on page 23](#)
  - ["Save the visible table data to a file" on page 24](#)
  - resize a column by clicking the edge and dragging to increase or decrease the size

5. To clear all items from the TL1 Response table, click the menu arrow and choose **Clear**.



# 19 Using a Telnet or SSH session to communicate with an NE

---

The NOC allows you to establish a Telnet session or a Secure Shell (SSH) session with an NE. Telnet or SSH is only available if your administrator has configured it using the Network Integrity Framework.

This section provides the following procedures for using a Telnet or SSH session to communicate with an NE:

- “Establish a Telnet or SSH session” on page 202
- “Change the appearance of a session window” on page 204
- “Save a Telnet or SSH session to file” on page 206
- “Send an ASCII file to an NE” on page 207
- “Edit text strings in a command” on page 207
- “Finding text” on page 209
- “Clear a session window screen” on page 210
- “Clear the scrollback buffer” on page 210
- “Restore the window to default properties” on page 210
- “Close the session window upon disconnecting” on page 210

You must log in to the NOC with a valid Network Integrity user ID and password with the correct roles and permissions assigned.

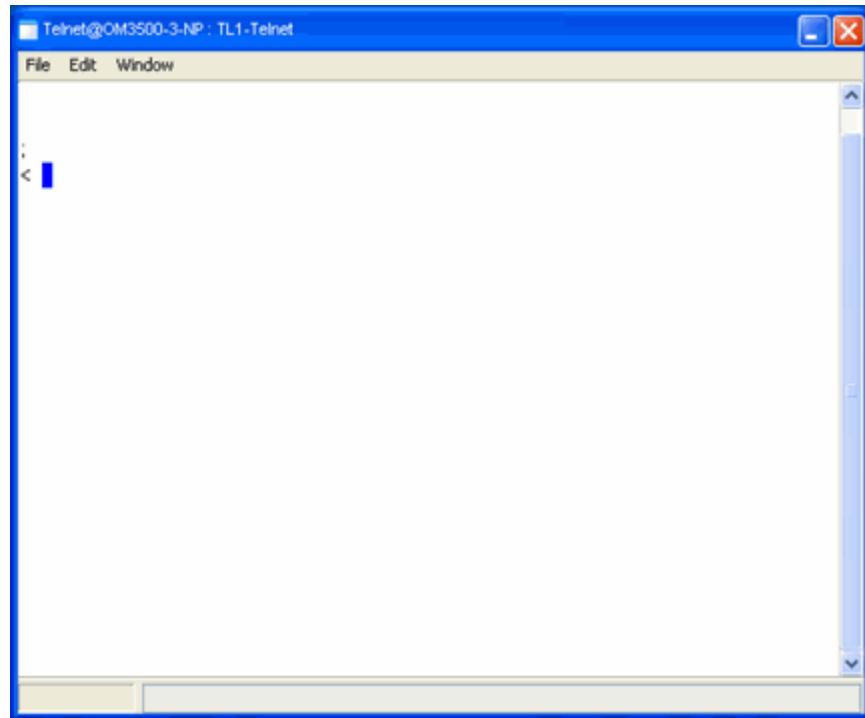
## 19.1 Establish a Telnet or SSH session

Use this procedure to establish a Telnet or SSH session with a network element.

1. In the Network Elements table or Topology view, right-click on an NE, choose **Maintenance**, and then choose the Telnet session or SSH session command.

Note: The command names that are displayed in the pop-up menu will depend on the Session Broker port configuration that was performed from the Network Integrity Framework. For example, if the name of the Session Broker port was configured as “**Telnet**”, the pop-up in the NOC will appear as “**Telnet**”.

The system displays a command window and establishes a session to the selected NE.



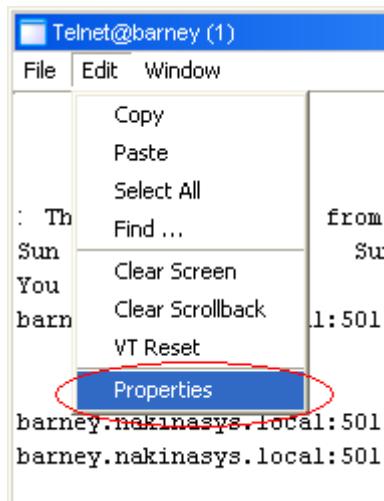
2. Enter commands as you would in any other Telnet client application window.  
**Note:** Depending on how your user account has been configured, you may be prevented from entering certain commands. Contact your system administrator if you experience problems executing certain commands.
3. If your NEs are TL1 NEs in a ring configuration, you can log in to other NEs in the same ring without terminating the current session by doing the following:
  - a. Press F12 to display a prompt.
  - b. At the prompt, type the ID of the NE to log into.  
If the NE is in the same ring and you are authorized to access it, Session Broker will log you in.  
You can also use the following commands at the prompt:
    - CTRL-B — Returns you to where you were before you pressed F12
    - CTRL-G — Displays the complete list of NEs that are available
    - CTRL-O — Displays a help menu
4. See also:
  - ["Change the appearance of a session window" on page 204](#)
  - ["Save a Telnet or SSH session to file" on page 206](#)
  - ["Send an ASCII file to an NE" on page 207](#)
  - ["Edit text strings in a command" on page 207](#)
  - ["Finding text" on page 209](#)

- “Clear a session window screen” on page 210
- “Clear the scrollback buffer” on page 210
- “Restore the window to default properties” on page 210
- “Close the session window upon disconnecting” on page 210

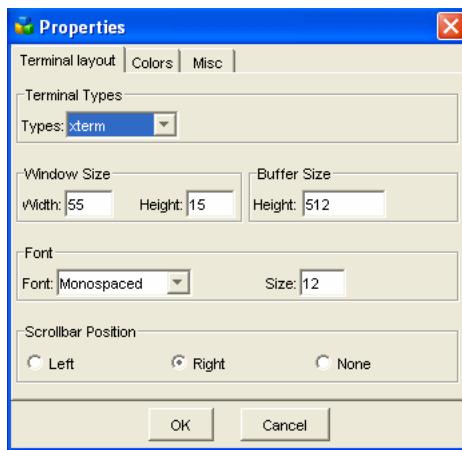
## 19.2 Change the appearance of a session window

Use this procedure to change display options to personalize the look and feel of the Telnet or SSH session. Each session window opened is adjusted separately.

1. In the session window, click **Edit**.
2. Click **Properties**.



The system displays the Properties window.



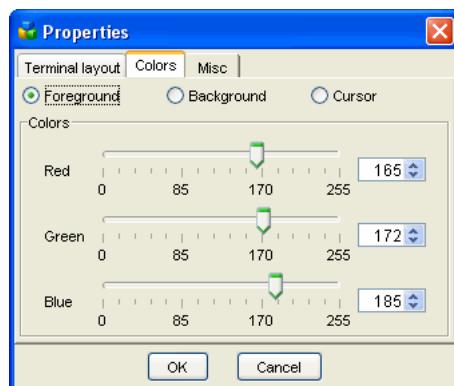
3. Click the **Terminal layout** tab.

4. Modify the fields in the **Terminal layout** tab as required. “[Display options for Terminal Layout](#)” on page 205 lists the display options for the **Terminal layout**.

**Table 19–1: Display options for Terminal Layout**

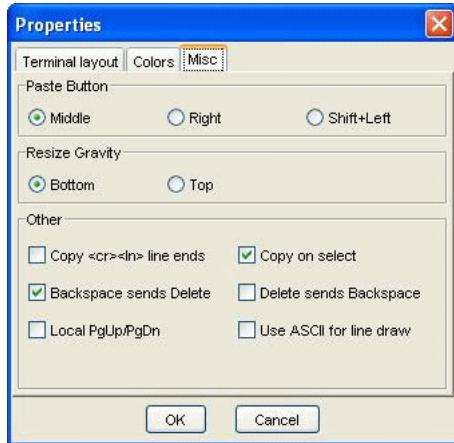
Display option	Description
Terminal Types	Select the drop-down list to choose a terminal type. Depending on the terminal type, commands may be interpreted differently.
Window Size	The window size is determined by height and width. Enter the desired height and width in the appropriate text boxes. Note that they are measured in terms of characters. For example, if the width were set to 80 this would mean that a line will hold up to 80 characters.
Buffer Size	The scrollback buffer size indicates how many lines of characters will be buffered in the window. When the number of lines exceeds this value, the oldest lines are deleted from the buffer. The contents of the buffer can also be manually cleared. See “ <a href="#">Clear the scrollback buffer</a> ” on page 210.
Font	Select the drop-down list to choose a font.
Size	Enter a font size for the text.
Scrollbar Position	Select the position of where you want the scrollbar to be placed, left or right. If you do not want to see the scrollbar, select None.

5. Click **OK** to apply the changes.
6. Click the **Colors** tab.
7. Select the attribute you want to change the color of. You can change the color of the **foreground**, **background**, or **cursor**.
8. Use the three meters to adjust to the desired color or enter a color number in the text fields.



9. Click **OK** to apply the changes.

10. Click the **Misc** tab.



11. Modify the fields on the **Misc** tab as required. ["Fields on the Misc tab" on page 206](#) provides details about the fields on the Misc tab.

**Table 19–2: Fields on the Misc tab**

Field	Description
Paste Button	Select a mouse button to use for the Paste function: Middle, Right, or Shift+Left.
Resize Gravity	Select an option to use for the fixed point on the screen when resizing: Bottom or Top.
Copy <cr><ln> line ends	Select this check box to include end-of-line characters when copying and pasting.
Copy on select	Select this check box to copy text that you have selected to the clipboard automatically.
Backspace sends Delete	Select this check box to map the Backspace key to the Delete operation.
Delete sends Backspace	Select this check box to map the Delete key to the Backspace operation.
Local PgUp/PgDn	Select this check box to activate the local Page Up and Page Down keys on the keyboard.
Use ASCII for line draw	Select this check box to use ASCII line-draw characters instead of drawing.

12. Click **OK** to apply the changes.

## 19.3 Save a Telnet or SSH session to file

Use this procedure to save the contents of a Telnet or SSH session to a file. This procedure is useful if you want to do debugging or analysis of the session data.

1. From the **File** menu of the session window, click **Capture to File**.

- The system displays the Save window.
2. Determine your next step:
- | If  | Then   |
|---|--|
| the file you want to save the contents of the session in exists         | locate the file  |
| the file you want to save the contents of the session in does not exist | create a new file by typing a file name in the <b>File name</b> text field |
3. Click **Save**.
  4. In the **File** menu, verify that the **Capture To File** command has a check mark beside it. This indicates that the NOC will save any further content to the specified file.
  5. To stop saving future text, in the **File** menu, clear the **Capture to File** command (has no check mark beside it).

## 19.4 Send an ASCII file to an NE

Use this procedure to send an ASCII file to an NE. The ASCII file will typically be made up of commands that are commonly used in a session. This procedure sends a set of commands to the NE where they will run automatically.

1. From the **File** menu of the session window, click **Send ASCII File**.  
The system displays the Open window.
2. Locate the file you want to open.
3. Click **Open**.  
The commands in the ASCII file are sent to the NE.

## 19.5 Edit text strings in a command

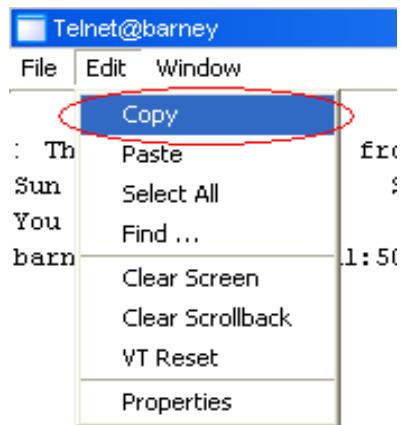
Use this procedure to copy, paste, and select text in a session window.

### To copy text

Use this procedure to copy text in a Telnet or SSH session window.

1. Select the text that you want to copy using the cursor in the session window.

2. In the **Edit** menu of the Telnet session window, click **Copy**.

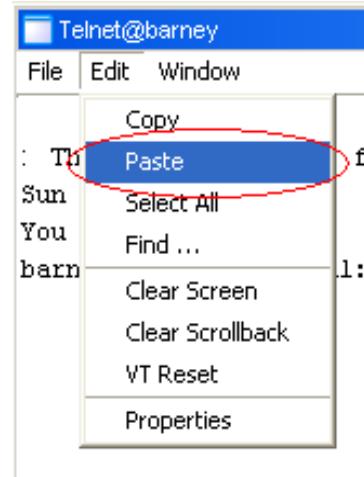


The selected text is copied.

#### To paste text

Use this procedure to paste text in a Telnet or SSH session window.

1. In the session window, click **Edit**.
2. Place the cursor where you want the previously-copied text to appear.
3. Click **Paste** to paste the previously-copied text.

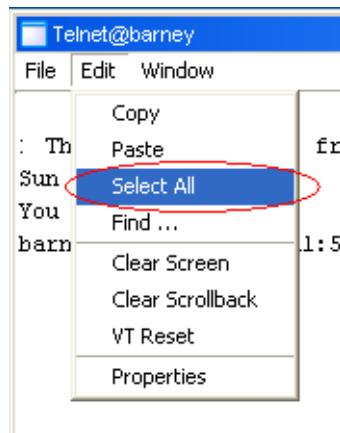


#### To select all text

Use this procedure to select all of the text in a Telnet or SSH session window.

1. In the session window, click **Edit**.

2. Click **Select All** to select all of the text in the current window.

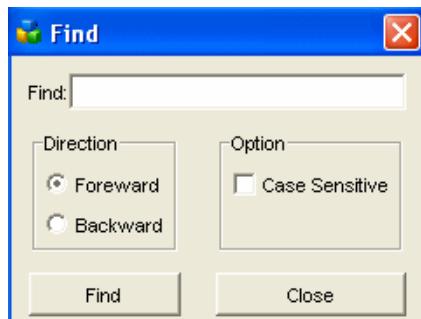


## 19.6 Finding text

Use this procedure to locate specific text in a Telnet or SSH session window.

1. From the session window, click **Edit**.
2. Click **Find....**

The system displays the Find window.



3. In the **Find** text field, type the text that you want to find.
4. Determine where you would like to search for the text that you want to find:

If	Then
you would like to search for text after the current cursor location	in the Direction box, select Forward
you would like to search for text before the current cursor location	in the Direction box, select Backward

5. In the **Option** box, select **Case Sensitive** to perform a case-sensitive search.
6. Click **Find**.

## 19.7 Clear a session window screen

Use this procedure to clear the screen in a Telnet or SSH session window.

1. In the session window, click **Edit**.
2. Click **Clear Screen** to delete all of the text in the current window.

The current session window becomes blank.

## 19.8 Clear the scrollback buffer

Use this procedure to clear the scrollback buffer in a Telnet or SSH session window. Clearing the scrollback buffer removes all text that is viewed by scrolling backwards in the session window.

1. In the session window, click **Edit**.
2. Click **Clear Scrollback** to delete all of the scrollback text.

The current session window has no scrollbar and all the previous scrollbar text has been cleared.

## 19.9 Restore the window to default properties

Use this procedure to reset a Telnet or SSH session window to its default properties.

1. In the session window, click **Edit**.
2. Click **VT Reset** to reset the settings.

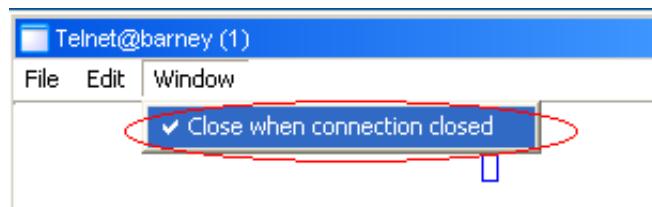
The current session window resets to the default properties.

## 19.10 Close the session window upon disconnecting

You can choose whether the session window will close or stay open when your session disconnects. A session disconnects when it times out or when you log out of the session.

Use this procedure to have a session window close upon disconnecting.

1. In the session window, click **Window**.
2. Check the **Close when connection closed** command.



3. To close the session, from the **File** menu of the session window, click **Close**.

### 19.10.1 Keep session window open upon disconnecting

Use this procedure to have a session window remain open upon disconnecting.

1. In the Telnet session window, click **Window**.
2. Clear the **Close when connection closed** command.
3. To close the session window, but keep the session active, from the **File** menu of the session window, click **Close**.

## 20 Transferring files to and from an NE

The NOC allows you to establish a File Transfer Protocol (FTP) or SSH File Transfer Protocol (SFTP) session to an NE. FTP or SFTP access is only available if your administrator has configured it using the Network Integrity Framework.

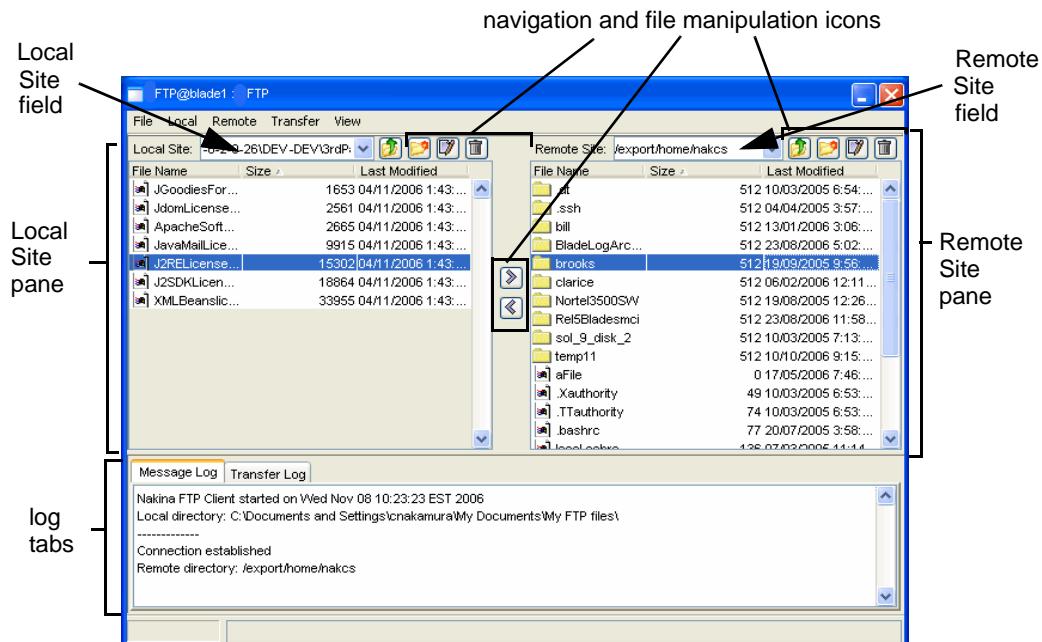
This section provides an overview (“[About the file transfer window](#)” on page 212) and the following procedures for transferring files:

- “[Launch the file transfer client](#)” on page 213
- “[Stop a connection attempt](#)” on page 213
- “[Disconnect from a session](#)” on page 214
- “[Manage files](#)” on page 214
- “[Transfer files to the remote site](#)” on page 217
- “[Transfer files from the remote site](#)” on page 219
- “[Change transfer configurations](#)” on page 220
- “[Hide or display the log tabs](#)” on page 220

You must log in to the NOC with a valid Network Integrity user ID and password with the correct roles and permissions assigned.

### 20.1 About the file transfer window

The following figure shows an example of the FTP and SFTP client.



[“Sections in the file transfer window” on page 213](#) describes the main sections of the file transfer window shown in the figure.

**Table 20–1: Sections in the file transfer window**

<b>Section</b>	<b>Description</b>
Local Site pane and field	The Local Site pane displays the location and contents of files on your computer. The Local Site field indicates the directory on your computer that you are located in.
Remote Site pane and field	The Remote Site pane displays the location and contents of files on the NE. The Remote Site field indicates the directory on the NE that you are located in.
Log tabs	There are two tabs that display a history of messages and transfers during a session: a message log tab and a transfer log tab. The message log tab shows the status of the session and any errors that occur. The transfer log tab lists the files that are being transferred and downloaded between sites. The file transfers can be sorted by host name, file name, status, size, or type.
Navigation and file manipulation icons	The navigation icons allow you navigate up through the directory structure on your computer and the NE. The file manipulation icons allow you to create, rename, delete, and transfer files or folders.

## 20.2 Launch the file transfer client

Use this procedure to access the file transfer client in the NOC.

1. In the Network Elements table or Topology view, right-click on an NE, choose **Maintenance**, and then choose the FTP session or SFTP session command.

Note: The command names that are displayed in the pop-up menu will depend on the Session Broker port configuration that was performed from the Network Integrity Framework. For example, if the name of the Session Broker port was configured as “**Secure FTP**”, the pop-up in the NOC would be “**Secure FTP**”.)

The system displays the session window and establishes a file transfer session to the selected NE.

## 20.3 Stop a connection attempt

Sometimes it can take a long time for a file transfer session to an NE to be established. Perform this procedure if you want to abort the connection process before it has been completed.

This procedure is only applicable during the period of time when the session is in the process of being established. If you want to disconnect after the session has been established, “[Disconnect from a session](#)” on page 214.

1. In the Network Elements table or Topology view, right-click on an NE, choose **Maintenance**, and then choose the FTP session or SFTP session command.

The system displays the session window.

2. In the session window, from the **File** menu, select **Stop Connection**.

The session window closes.

Note: After the session has been established, the **Stop Connection** command is disabled.

## 20.4 Disconnect from a session

There are two ways to disconnect from an established file transfer session. You can click the close button on the window, or perform the following procedure.

This procedure is only applicable for an established connection. To abort the connection process before it has been established, “[Stop a connection attempt](#)” on page 213.

1. In the session window, in the **File** menu, select the **Disconnect** command.  
The system displays a confirmation window.
2. Click **Yes** to confirm the action.  
The session closes.

## 20.5 Manage files

The file transfer client allows you to navigate through and manage all of the directories on your computer.

### 20.5.1 Sort files

You can sort the current directory by file name, size, and last modified. To sort on an attribute, click on the column heading for the attribute in either the Local Site pane or the Remote Site pane.

File Name	Size	Last Modified
cacheHttp	0	26/08/2005 9:34...
chainsaw.bat	184	26/08/2005 1:15...
license.bea	0993	26/08/2005 1:15...
run.bat	1184	26/08/2005 1:15...
runFtpClient...	221	26/08/2005 1:15...
runHttpClien...	439	26/08/2005 1:15...
storm	5891	23/08/2005 4:15...

### 20.5.2 Move up a folder

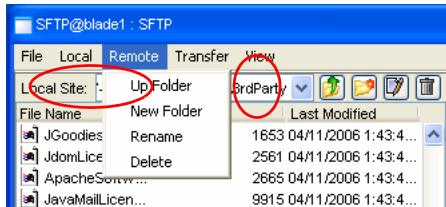
Use this procedure to navigate up a folder from the current folder.

1. Perform one of the following steps:
  - a. Determine which site to navigate.

If	Then
you want to navigate the local site	In the <b>Local</b> menu, select <b>Up Folder</b> .
you want to navigate the remote site	In the <b>Remote</b> menu, select <b>Up Folder</b> .

The current folder moves up one level.

- b. Click on the Go one directory up icon in the Local Site pane or the Remote Site pane.



### 20.5.3 Create a new folder

Use this procedure to create a new folder in the current directory. There are two ways to create a new folder:

- using the menu of the session window
- using the file manipulation icon

#### Using the menu of the session window

1. Determine which site to navigate.
- a.

If	Then
you want to navigate the local site	From the <b>Local</b> menu, select <b>New Folder</b> .
you want to navigate the remote site	From the <b>Remote</b> menu, select <b>New Folder</b> .

- b. Go to [Step 3](#).

#### Using the file manipulation icon

2. Click on the New Folder icon in the Local Site pane or the Remote Site pane.



The system displays an Input window and prompts for the name of the new folder.

3. In the Input window, type the name of the new folder.
  4. Click **OK**.
- A new folder with the given name is created.

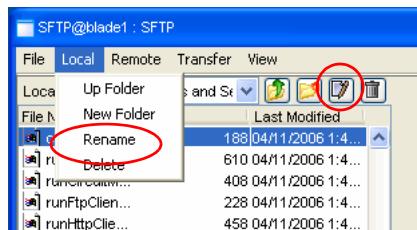
### 20.5.4 Rename a file or folder

Use this procedure to rename a file or folder in the current directory.

1. In either the Local Site pane or the Remote Site pane, click on a file or folder.
2. Perform one of the following steps:
  - a.

If	Then
you want to rename a file or folder on the local site	From the <b>Local</b> menu, select <b>Rename</b> .
you want to rename a file or folder on the remote site	From the <b>Remote</b> menu, select <b>Rename</b> .

- b. Click on the Rename icon in the Local Site pane or the Remote Site pane.



The system displays the Input window.

3. In the Input window, type the new name of the file or folder.
4. Click **OK**.

The file or folder is renamed.

## 20.5.5 Delete a file or folder

You can delete a file or folder by using:

- the delete command
- the delete icon
- the option bar

### Prerequisites

Before performing this procedure the folder must be empty.

### Delete a file or folder using the Delete command

Use this procedure to delete a file or folder using the **Delete** command.

1. Select the file or folder to delete. Use **Shift-click** or **Ctrl-click** to select multiple files.

2. Determine which site the selected file or folder resides on.

If	Then
you want to delete a file or folder on the local site	From the <b>Local</b> menu, select <b>Delete</b> .
you want to delete a file or folder on the remote site	From the <b>Remote</b> menu, select <b>Delete</b> .

The system displays the Delete window and prompts for confirmation.

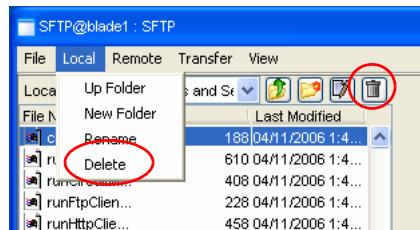
3. Click **Yes** to confirm the action.

The selected file or folder is deleted.

### Delete a file or folder using the delete icon

Use this procedure to delete a file or folder using the delete icon.

1. Select the file or folder to delete. Use **Shift-click** or **Ctrl-click** to select multiple files.
2. Click on the Delete icon in the Local Site pane or the Remote Site pane.



### Delete a file or folder using the option bar

Use this procedure to delete a file or folder using the option bar.

1. Right-click the selected file and select **Delete**.



The system displays a confirmation prompt.

2. Click **Yes** to confirm the deletion.
- The selected file or folder is deleted.

## 20.6 Transfer files to the remote site

You can transfer files from the local site to the remote site using:

- the Upload command
- the upload icon

- the option bar

### 20.6.1 Transfer files to the remote site using the Upload command

Use this procedure to transfer files to the remote site using the **Upload** command.

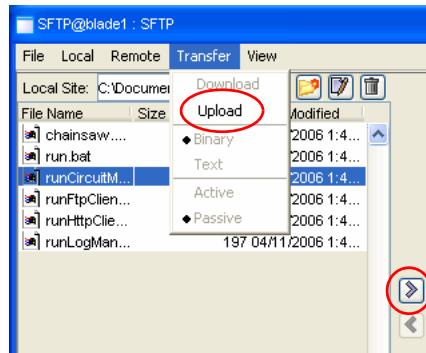
1. In the Local Site pane, select the file or folder to upload. Use **Shift-click** or **Ctrl-click** to select multiple files.
2. From the Transfer menu, select **Upload**.

The selected file or files are uploaded to the current directory. The log pane shows the upload activity.

### 20.6.2 Transfer files to the remote site using the upload icon

Use this procedure to transfer files to the remote site using the upload icon.

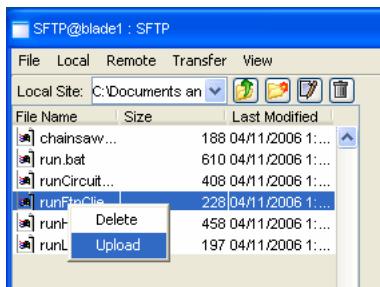
1. In the Local Site pane, select the file or folder to upload. Use **Shift-click** or **Ctrl-click** to select multiple files.
2. Click the upload icon.



### 20.6.3 Transfer files to the remote server using the option bar

Use this procedure to transfer files to the remote site using the option bar.

1. In the Local Site pane, select the file or folder from which to upload. Use **Shift-click** or **Ctrl-click** to select multiple files.
2. Right-click the selected file and select **Upload**.



The selected file or files are uploaded to the current directory. The log pane shows the upload activity.

## 20.7 Transfer files from the remote site

You can transfer files from the remote site to the local site using:

- the Download command
- the download icon
- the option bar

### 20.7.1 Transfer files from the remote site using the Download command

Use this procedure to transfer files from the remote site to the local site using the **Download** command.

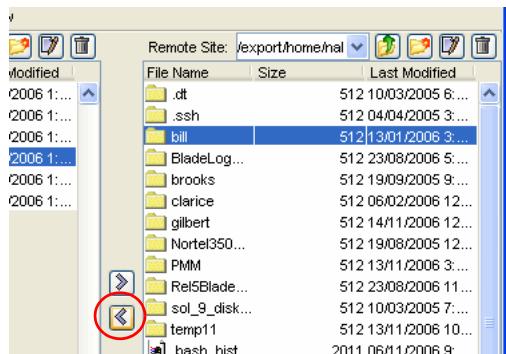
1. In the Remote Site pane, select the file or folder to download. Use **Shift-click** or **Ctrl-click** to select multiple files.
2. In the client window, click **Transfer**.
3. Click **Download**.

The selected folder or file is downloaded to the current directory. The log pane shows the download activity.

### 20.7.2 Transfer files from the remote site using the download icon

Use this procedure to transfer files from the remote site to the local site using the download icon.

1. In the Remote Site pane, select the file or folder to download. Use **Shift-click** or **Ctrl-click** to select multiple files.
2. Click the Download icon that is between the Local Site pane and the Remote Site pane.



### 20.7.3 Transfer files from the remote site using the option bar

Use this procedure to transfer files from the remote site using the option bar.

1. In the Remote Site pane, select the file or folder to download. Use **Shift-click** or **Ctrl-click** to select multiple files.
2. Right-click the selected file and select **Download**.

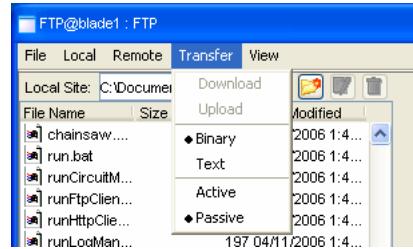
The selected file or files are downloaded to the current directory. The log pane shows the download activity.



## 20.8 Change transfer configurations

Use this procedure to change the transfer configurations of an FTP session. Transfer configurations are set to match the NE that is being communicated with. This procedure is not applicable for SFTP sessions.

1. In the client window, click **Transfer**.
2. Click the options that you want to change to. The current configurations are marked with bullets.



The following transfer options are available:

- Binary, which transfers data in single-byte units. Binary transfer is used for images, data files, and word processing documents.
- Text, which transfers data as an ASCII file. Text transfer is used for text-only files.

The following transfer modes are available:

- Active, which sets the FTP server to make connections with high ports on the client. Connections may be blocked by a firewall on the client side.
- Passive, which sets the FTP server to make connections with high ports on the server. Connections may be blocked by a firewall on the server side.

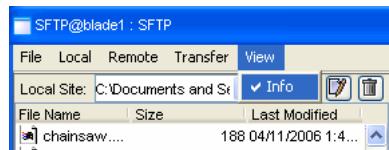
## 20.9 Hide or display the log tabs

The log tabs can be hidden or displayed.

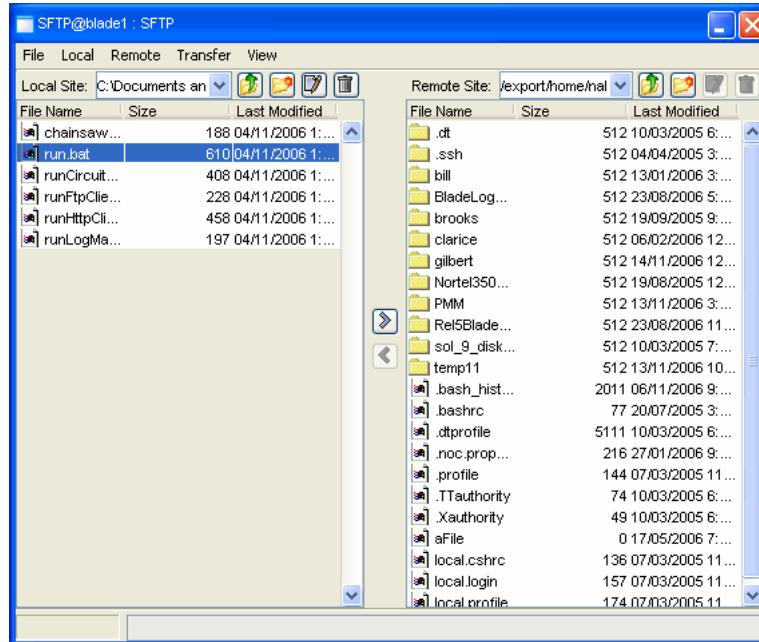
### 20.9.1 Hide the log tabs

If the log tabs are being displayed in the client window, perform this procedure to hide them.

1. In the client window, from the **View** menu, select **Info**.



The log tabs disappear from the client window and the check mark is removed from the Info command.

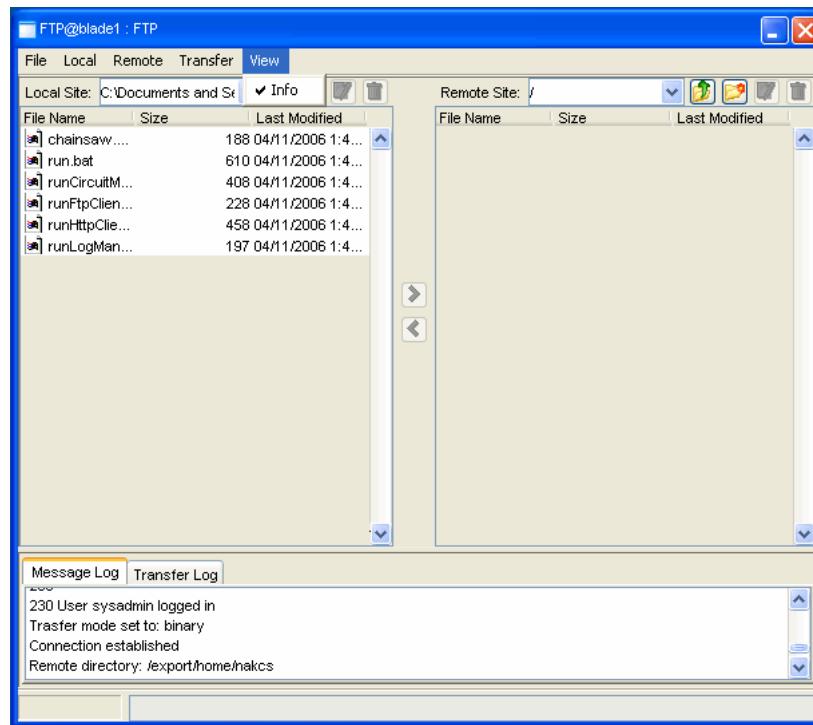


### 20.9.2 Display the log tabs

If the log tabs are currently hidden in the client window, perform this procedure to display them.

1. In the client window, from the **View** menu, select **Info**.

The log tabs are displayed and a check mark appears beside the Info command.



# 21 Troubleshooting

The following table provides information on common NOC issues.

Problem	Solution
While using the NOC you do not see menu items, tabs or buttons that are described in this documentation.	Your administrator has not assigned the required permission to user account roles.
A button that is normally available to you now appears grayed out.	This means that you have the role and permission to perform the action, but not for the NE group that you are currently dealing with. You must assign the NE group in question to the role that corresponds to the action you are trying to perform.
The NOC takes a long time to open.	The time it takes to open the NOC is dependent on the size of the network, the power and speed of your computer, and other factors. For ways to speed up the log in process, see <a href="#">"Set preferences" on page 25</a> .
After a number of invalid login attempts you are locked out of the NOC.	The number of invalid login attempts is configurable through the Network Integrity Framework. If you are locked out of the NOC after a number of login attempts, it is because this feature has been configured for your user ID. Speak to your network administrator for more information.
After a period of inactivity your NOC session is terminated.	The amount of time a NOC session can sit idle before a user is automatically logged off is configurable through the Network Integrity Framework. If your session is terminated after a period of inactivity, it is because this feature has been configured for your user ID. Speak to your network administrator for more information.
The navigation panel is too small to see groups, and the "Find Network Elements" field is too small to enter text in.	For a temporary fix, resize the navigation panel down and to the right. For a permanent fix, increase the resolution setting on your monitor to 1280x1024 or greater.
An "Error in TL1 Command and Control" message is displayed when you start the NOC that indicates that the EnableVendorModels.xml file cannot be found.	<p>This means that your administrator selected the Command and Control plugin when the NOC was installed but did not configure it.</p> <p>You can click Close to use other NOC functionality, but you cannot use the Command and Control plugin until it is configured.</p>

## Appendix A: NE icons in the Topology view

The following table provides a list of the industry standard icons used by the NOC to represent the NE type in the Topology view.

Access Equipment		Switching Line Terminating Equipment 1	
Edge Cell Regenerator		Switching Line Terminating Equipment 2	
Edge Cross-Connect		Switching MUX 1	
Edge End Office		Switching MUX 2	
Edge Gateway		Switching STP 1	
Edge Hub		Switching STP 2	
Edge Line Terminating Equipment		Switching Toll Gateway 1	
Edge Mux		Switching Toll Gateway 2	
Edge Ratio Cell Site Equipment		Switching Toll Tandem1	
Edge Wireless Edge		Switching Toll Tandem2	
IP Access		Transport Equipment	
IP Bridge		Transport Access1	
IP Equipment		Transport Access2	
IP Hub		Transport ADM	

IP LAN Regenerator		Transport ADM1	
IP Line Terminating Equipment		Transport ADM2	
IP MUX		Transport Amplifier	
IP Router		Transport Cross-Connect	
IP Signaling Gateway		Transport Cross-Connect1	
IP STP		Transport Cross-Connect2	
IP Switch		Transport DWDM Optical	
IP Switch Router		Transport Hub1	
IP Traffic Gateway		Transport Hub2	
Switch Equipment		Transport LTE	
Switch Cross-Connect		Transport LTE 1	
Switching ATM		Transport LTE 2	
Switching DMS		Transport Regenerator	
Switching End Office1		Transport SONET SDH	
Switching End Office2		Transport Traffic Gateway (GNE)	
Switching Hub1		Unknown NE Type	

NE icons in the Topology view

Switching Hub2

