

# HP Network Node Manager i-Series Software

For the Windows®, HP-UX, Linux, and Solaris operating systems

Software Version: NNMi 8.1x patch 5 (8.13)

---

[Online Help: Help for Operators](#)

Document Release Date: August 2009

Software Release Date: August 2009



## PDF Version of NNMi Online Help

This document is a PDF version of the NNMi online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format.

**Note:** Some topics do not convert properly to PDF format. You may encounter formatting problems or unreadable text in certain document locations. Those problem topics can be successfully printed from within the online help.

## Legal Notices

### Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

### Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

For information about third-party license agreements, see the license-agreements directory on the product installation media.

### Copyright Notices

© Copyright 2009 Hewlett-Packard Development Company, L.P.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). Portions Copyright © 1999-2003 The Apache Software Foundation. All rights reserved.

This product includes ASM Bytecode Manipulation Framework software developed by Institute National de Recherche en Informatique et Automatique (INRIA). Copyright © 2000-2005 INRIA, France Telecom. All Rights Reserved.

This product includes Commons Discovery software developed by the Apache Software Foundation (<http://www.apache.org/>). Copyright © 2002-2009 The Apache Software Foundation. All Rights Reserved.

This product includes Netscape JavaScript Browser Detection Library software, Copyright © Netscape Communications 1999-2001

This product includes Xerces-J xml parser software developed by the Apache Software Foundation (<http://www.apache.org/>). Copyright © 1999-2002 The Apache Software Foundation. All rights reserved.

This product includes software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>). Xpp-3 Copyright © 2002 Extreme! Lab, Indiana University. All rights reserved.

### Trademark Notices

DOM4J® is a registered trademark of MetaStuff, Ltd.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Java™ is a US trademark of Sun Microsystems, Inc.

Oracle® is a registered trademark of Oracle Corporation and/or its affiliates.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

### Oracle Technology — Notice of Restricted Rights

Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing

restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

For the full Oracle license text, see the license-agreements directory on the NNMi product DVD.

## Table of Contents

---

<b>PDF Version of NNMi Online Help</b> .....	<b>2</b>
<b>Legal Notices</b> .....	<b>3</b>
<b>Table of Contents</b> .....	<b>5</b>
<b>Using Network Node Manager</b> .....	<b>13</b>
<b>Accessing NNM 6.x and 7.x Features</b> .....	<b>14</b>
<b>Learning Your Network Inventory</b> .....	<b>15</b>
Filter Views by Node or Interface Group.....	16
Nodes View (Inventory).....	16
Interfaces View (Inventory).....	17
IP Addresses View (Inventory).....	19
IP Subnets View (Inventory).....	19
VLANs View (Inventory).....	20
Layer 2 Connections View.....	21
Nodes By Device Category View (Inventory).....	21
Interfaces by IfType View (Inventory).....	22
Custom Nodes View (Inventory).....	23
Custom Interfaces View.....	23
Router Redundancy Group View (NNMi Advanced).....	24
Custom IP Addresses View (Inventory).....	24
Node Groups View (Inventory).....	25
Interface Group View (Inventory).....	25
Management Stations View (Inventory).....	26
<b>Accessing Device Details</b> .....	<b>27</b>
Node Form.....	28
Node Form: General Tab.....	32
Node Form: IP Addresses Tab.....	33
Node Form: Interfaces Tab.....	33
Node Form: VLAN Ports Tab.....	34
VLAN Port Form.....	34
Node Form: Ports Tab.....	35
Node Form: Capabilities Tab.....	35
Node Capabilities Provided by NNMi.....	36

---

---

Node Capability Form .....	38
Node Form: Custom Attributes Tab .....	39
Node Custom Attributes Form .....	39
Node Form: Node Groups Tab .....	39
Node Form: Component Health Tab .....	40
Node Component Form .....	40
Node Component Form: Health Attributes Tab .....	42
Health Attribute Form .....	42
Node Component Form: Incidents Tab .....	44
Node Component Form: Status Tab .....	44
Node Component Form: Conclusions Tab .....	45
Node Form: Diagnostics Tab (NNM iSPI NET) .....	46
Node Diagnostic Results Form (Flow Run Result) (NNM iSPI NET) .....	47
Node Form: Incidents Tab .....	48
Node Form: Status Tab .....	48
Node Form: Conclusions Tab .....	49
Node Form: Registration Tab .....	50
SNMP Agent Form .....	50
SNMP Agent Form: Status Tab .....	54
SNMP Agent Form: Conclusions Tab .....	54
SNMP Agent Form: Incidents Tab .....	55
SNMP Agent Form: Registration Tab .....	55
Device Profile Form .....	56
Device Family Form .....	58
Device Vendor Form .....	58
Device Category Form .....	59
Device Profile Author Form .....	59
Interface Form .....	60
Interface Form: General Tab .....	63
Interface Form: IP Addresses Tab .....	64
Interface Form: VLAN Ports Tab .....	64
Interface Form: Link Aggregation Tab (NNMi Advanced) .....	65
Interface Form: Capabilities Tab .....	66
Interface Capabilities Provided by NNMi .....	67
Interface Capability Form .....	69

---

---

Interface Form: Custom Attributes Tab .....	69
Interface Custom Attributes Form .....	69
Interface Form: Interface Groups Tab .....	70
Interface Form: Performance Tab (NNM iSPI Performance for Metrics) .....	70
Interface Form: Incidents Tab .....	71
Interface Form: Status Tab .....	72
Interface Form: Conclusions Tab .....	73
Interface Form: Registration Tab .....	73
IP Address Form .....	73
IP Address Form: Incidents Tab .....	75
IP Address Form: Status Tab .....	75
IP Address Form: Conclusions Tab .....	76
IP Address Form: Capabilities Tab .....	77
IP Address Capabilities Provided by NNMi .....	77
IP Address Capability Form .....	78
IP Address Form: Registration Tab .....	78
Router Redundancy Group Form (NNMi Advanced) .....	79
Router Redundancy Group Form: Router Redundancy Members Tab (NNMi Advanced) .....	80
Router Redundancy Member Form (NNMi Advanced) .....	80
Router Redundancy Member Form: Tracked Objects Tab (NNMi Advanced) .....	83
Tracked Objects Form (NNMi Advanced) .....	84
Router Redundancy Group Form: Virtual IP Addresses Tab (NNMi Advanced) .....	84
Virtual IP addresses Form (NNMi Advanced) .....	85
Router Redundancy Group Form: Incidents Tab (NNMi Advanced) .....	85
VLAN Form .....	86
VLAN Form: Ports Tab .....	86
Port Form .....	87
Port Form: VLANs Tab .....	87
Node Group Form .....	88
Node Group Form: Device Filters Tab .....	89
Node Device Filter Form .....	89
Node Group Form: Additional Filters Tab .....	90
Node Group Form: Additional Nodes Tab .....	90
Additional Node Form .....	91
Node Group Form: Child Node Groups Tab .....	92

---

---

Node Group Hierarchy (Child Node Group) Form.....	92
Node Group Form: Status Tab.....	93
Interface Group Form.....	94
Interface Group Form: IfType Filters Tab.....	95
IfType Filter Form.....	95
IfType (Interface Type) Form.....	96
Interface Group Form: Additional Filters Tab.....	96
Management Station Form.....	97
<b>Viewing Maps (Network Connectivity).....</b>	<b>98</b>
Node Group Maps.....	99
Navigating within a Node Group Map.....	100
Position Nodes on a Node Group Map.....	101
Node Group Overview Map.....	101
Network Overview Map.....	102
Networking Infrastructure Devices Map.....	102
Routers Map.....	103
Switches Map.....	103
Display the Layer 2 Neighbor View.....	104
Layer 2 Connection Form.....	106
Layer 2 Connection Form: Interfaces Tab.....	107
Layer 2 Connection Form: Incidents Tab.....	108
Layer 2 Connection Form: Status Tab.....	108
Layer 2 Connection Form: Conclusions Tab.....	109
Layer 2 Connection Form: Link Aggregation Tab (NNMi Advanced).....	109
Layer 2 Connection Form: Registration Tab.....	111
Display the Layer 3 Neighbor View.....	112
IP Subnet Form.....	113
IP Subnet Form: IP Addresses Tab.....	114
IP Subnet Form: Registration Tab.....	114
Path Between Two Nodes that Have IPv4 Addresses.....	114
Path Calculation Rules.....	116
Path View Limitations.....	117
Investigate Errors and Performance Issues.....	118
Enhanced Path View (NNMi Advanced).....	118
<b>Monitoring Devices for Problems.....</b>	<b>120</b>

---



---

Monitor with Table Views .....	120
Critical Interfaces View .....	120
Critical Nodes View .....	121
Critical Component View .....	121
Non-Normal Interfaces View .....	122
Non-Normal Nodes View .....	122
Non-Normal Router Redundancy Group View (NNMi Advanced) .....	123
Not Responding Address View .....	124
Nodes by Status View .....	124
Interfaces by Status View .....	125
Interfaces by Administrative State View .....	125
Interfaces by Operational State View .....	126
IP Addresses by State View .....	126
Component by Status View .....	127
Interface Performance View (NNM iSPI Performance for Metrics) .....	127
Node Groups View (Monitoring) .....	128
Monitor with Map Views .....	128
Watch Status Colors .....	129
Determine Problem Scope .....	129
Access a Problem Device .....	129
Access Node Details .....	130
Access All Related Incidents .....	130
<b>Monitoring Incidents for Problems .....</b>	<b>132</b>
Organize Your Incidents .....	133
Incident Form .....	134
Incident Form: General Tab .....	135
Incident Form: Correlated Parents Tab .....	142
Incident Form: Correlated Children Tab .....	142
Incident Form: Custom Attributes Tab .....	142
Custom Incident Attribute Form .....	143
Custom Incident Attributes Provided by NNMi (for Operators) .....	143
Incident Form: Diagnostics Tab (NNM iSPI NET) .....	147
Incident Diagnostic Results Form (Flow Run Result) (NNM iSPI NET) .....	147
Incident Form: Registration Tab .....	148
Manage Incident Assignments .....	149

---

---

Own Incidents.....	149
Assign Incidents.....	150
Unassign Incidents.....	150
Keep Your Incidents Up to Date.....	151
About the Incident Lifecycle.....	154
Track an Incident's Progress.....	157
Display a Map from an Incident.....	158
Island Node Group Map.....	158
Incident Views Provided by NNMi.....	159
My Open Incidents View.....	160
Key Incident Views.....	160
Open Key Incidents View.....	161
Unassigned Open Key Incidents View.....	163
Open Key Incidents by Severity View.....	164
Open Key Incidents by Priority View.....	165
Open Key Incidents by Category View.....	166
Open Key Incidents by Family View.....	167
Closed Key Incidents View.....	168
Key Incidents by Lifecycle State View.....	169
Root Cause Incidents.....	170
Root Cause Incidents View.....	171
Open Root Cause Incidents View.....	171
Service Impact Incidents View.....	172
Stream Correlation Incidents View.....	172
Incidents by Family View.....	173
Custom Incidents View.....	173
NNM 6.x/7.x Events View.....	174
NNM 6.x/7.x Events by Category View.....	174
SNMP Traps View.....	175
SNMP Traps by Family View.....	175
<b>Analyze Trap Information.....</b>	<b>176</b>
<b>Investigate and Diagnose Problems.....</b>	<b>177</b>
Verify Device Configuration Details.....	177
View the Monitoring Configuration Details.....	178
Verify Current Status of a Device.....	180

---

---

Interpret Root Cause Incidents.....	181
Address Disabled.....	182
Address Not Responding.....	182
Aggregator Interface Degraded (NNMi Advanced).....	183
Aggregator Interface Down (NNMi Advanced).....	184
Aggregator Connection Degraded (NNMi Advanced).....	185
Aggregator Connection Down (NNMi Advanced).....	185
Buffer has Insufficient Capacity or is Malfunctioning.....	186
Connection Down.....	186
Connection Partially Unresponsive.....	187
CPU Utilization is too High.....	188
Fan is Malfunctioning.....	188
Interface Down.....	188
Interface Disabled.....	189
Interface Unmanageable.....	190
Remote Site Containing Node <Source Node Name> is Unreachable.....	191
Memory has Insufficient Capacity or is Malfunctioning.....	192
Node Down.....	192
Node or Connection Down.....	194
Non-SNMP Node Unresponsive.....	195
Number of SNMP Traps Persisted in the Database has Reached or Exceeded Trap Limit.....	195
Power Supply is Malfunctioning.....	196
SNMP Agent Not Responding.....	196
Temperature Sensor is Out of Range.....	196
Voltage is Out of Range.....	197
Interpret Service Impact Incidents.....	197
Primary Device in Router Redundancy Group Switched (NNMi Advanced).....	198
No Primary Device in Router Redundancy Group (NNMi Advanced).....	198
Multiple Primary Devices in Router Redundancy Group (NNMi Advanced).....	198
No Secondary Device in Router Redundancy Group (NNMi Advanced).....	198
Multiple Secondary Devices in Router Redundancy Group (NNMi Advanced).....	199
Router Redundancy Group Degraded (NNMi Advanced).....	199
Interpret Threshold Incidents (NNM iSPI Performance for Metrics).....	199
Input and Output Utilization Incidents (NNM iSPI Performance for Metrics).....	200
Input and Output Error Rate Incidents (NNM iSPI Performance for Metrics).....	201

---

---

Input and Output Discard Rate Incidents (NNM iSPI Performance for Metrics) .....	202
Find a Node.....	203
Find the Attached Switch Port .....	204
Display End Nodes Attached to a Switch.....	204
Test Node Access (Ping).....	206
Find the Route (traceroute).....	206
Establish Contact with a Node (telnet).....	207
Check Status Details for a Node Group.....	208
Accessing NNM 6.x and 7.x Features .....	209
<b>Checking the Status of NNMi .....</b>	<b>211</b>
<b>Appendix A: Glossary Terms .....</b>	<b>212</b>
<b>Appendix B: Index.....</b>	<b>214</b>

## Using Network Node Manager

NNMi enables you to quickly detect, isolate, and troubleshoot abnormal network behavior. Using NNMi, you can also record what has been done to date to troubleshoot or resolve a problem.

The following table describes some of the ways that NNMi assists in making your job easier and the help topics that would be most valuable for accomplishing those tasks.

Task	Help Topic
Rapidly detect, isolate, and correct the problem	<a href="#">"Monitoring Devices for Problems" (on page 120)</a> and <a href="#">"Investigate and Diagnose Problems" (on page 177)</a>
Annotate information for future diagnosis	<a href="#">"Accessing Device Details" (on page 27)</a>
Look for historical information to proactively monitor the network	<a href="#">"Monitoring Incidents for Problems" (on page 132)</a>
View an inventory of what is being managed	<a href="#">"Learning Your Network Inventory" (on page 15)</a>

## Accessing NNM 6.x and 7.x Features

Your NNMi administrator might configure NNMi so that you are able to view incidents that are being forwarded from an NNM 6.x or 7.x management station.

If your NNMi administrator has configured any NNM 6.x or 7.x management stations, you are able to view this information using the **Inventory** workspace. The **Management Stations** view in the **Inventory** workspace is useful for identifying all of the NNM 6.x or 7.x management stations that might be forwarding incidents to your NNMi incident views. See "[Management Stations View \(Inventory\)](#)" (on page 26) for more information.

If an NNM 6.x or 7.x management station has been configured, you are also able to access the following NNM 6.x or 7.x features from the NNMi **Actions** menu:

**Note:** You can only launch the 6.x/7.x ovw action if ovw is running on the NNM 6.x/7.x management station.

From Incident Views

- **Actions** → **6.x/7.x Neighbor View**
- **Actions** → **6.x/7.x Details**
- **Actions** → **6.x/7.x ovw**

From Management Station Views

- **Actions** → **6.x/7.x Home Base**
- **Actions** → **6.x/7.x ovw**
- **Actions** → **6.x/7.x Launcher**
- **Actions** → **SNMP Viewer**
- **Actions** → **Alarms**


**Note:** You can only access NNM 6.x/7.x features by selecting incidents generated from NNM 6.x/7.x events.


## Learning Your Network Inventory

After NNMi discovers your network (or rediscovers it on a regular basis), you have several options for exploring what was discovered. See up-to-date information for each of the following:


### Types of Views Provided by NNMi

Object Type	Purpose
Nodes	Identify all nodes being managed.
Network interfaces	Identify all network interfaces being managed, their associated node, and any interfaces that are disabled or otherwise unavailable.
IP addresses	Identify the IP addresses associated with each node being managed.
IP Subnets	Identify all of the networks within NNMi's management domain. Browse for large and small subnets.
VLANs	Identify all of the switch port VLANs configured in your network environment. NNMi ignores VLAN-1, but higher numbered VLANs are discovered.

Within any table view, you can quickly view a few additional properties of your network devices. To do so, click the  Quick View icon within the row representing a network object. Quick View provides information at a glance for some pre-determined object attributes.

Forms are a way to gain a more in depth understanding of a particular object instance. To view the form for the object's attributes, from a table view, click the  Open icon that precedes the object information. The form containing the information for the object's attributes appears.

To view all of the text for an attribute value within the form, click the attribute label of interest. The attribute value appears in a popup window. This option is useful when not all of the text is viewable within the form field.

You can also access another form from the current one for any related objects. Related objects in a form appear as lookup fields. Each  Lookup field includes a drop-down menu that lets you open the form for that object.

You can filter views using pre-defined Node Groups and Interface Groups. Select a filter by using the  drop-down filter selection. See [Filter by Node or Interface Group](#) for more information about filters.

In the form for that object, you can view or edit the information for the selected object as described in [Working with Objects](#).

### Related Topics

["Nodes View \(Inventory\)" \(on page 16\)](#)

["Interfaces View \(Inventory\)" \(on page 17\)](#)

["IP Addresses View \(Inventory\)" \(on page 19\)](#)

["IP Subnets View \(Inventory\)" \(on page 19\)](#)

## Filter Views by Node or Interface Group

When monitoring your network, you might be interested in only viewing information for a particular set of nodes or interfaces. Your network administrator is able to group sets of nodes or interfaces into node or interface groups. An example of a Node Group could be all important Cisco routers, or all routers in a particular building. As another example, all interfaces used for Voice-Over-IP might be grouped together in a Node Group.

**Note:** Node Group filters are not available for the **NNM 6.x/7.x Events** view.

You can filter the following kinds of views by Node Group:

- Node views
- Interface views
- IP address views
- Incident views

You can filter the following views by interface group:

- Interface views
- IP address views

If a view includes filtering by both node and interface groups, NNMi lists the Node Groups first, followed by all of the interface groups. Each list appears in alphabetical order.

### To filter a view by node or interface group:


1. Navigate to the view of interest
  - a. From the workspace navigation panel, select the workspace that contains the view you want to use; for example **Inventory**.
  - b. Select the view of interest; for example **Nodes**.
2. In the  group selector drop-down list, select the Node or Interface Group you want to use as a filter.

## Nodes View (Inventory)

**Tip:** See "[Node Form](#)" (on page 28) for more details about the node attributes that appear in this view's column headings.

The Nodes view in the Inventory workspace is useful for identifying all of the nodes being managed by NNMi.

For each node displayed, you can identify its overall status (for example, **Normal**, **Warning**, **Minor**, **Major**, **Critical**, or **Unknown**), device category (for example, **Switch**), name, hostname, management address, system location (the current value of the sysLocation MIB variable), device profile, date indicating the last time the node status was modified, and any notes included for the node.

**Note:** Your NNMi administrator is able to delete nodes and other objects from the NNMi database. Any node that has been deleted appears as a transparent icon on the map until the map is refreshed using the  **Refresh** icon. After **Refresh**, the deleted node is removed from the map. NNMi does not automatically refresh the connectivity or set of nodes in a map view, except on the Network Overview map.

Node views are useful for quickly identifying items described in the following table.



## Uses for Nodes Views

Use	Description
View all problem nodes	Sort the view by <b>Status</b> so that you can be quickly alerted to existing and potential problems.  You can also access the <b>Critical Nodes</b> view provided by NNMi. See " <a href="#">Critical Nodes View</a> " (on page 121) for more information.
View all device types being managed	Sort the view by the <b>Device Profile</b> attribute.
Identify whether the problem can be isolated to a particular area of your network	Sort the view by <b>System Location</b> . This is the current value of the sysLocation MIB variable.
View address and subnet information associated with a selected node to better determine the scope of the problem	From the <b>Nodes</b> view, open the <b>Node</b> form. Select the <b>Addresses</b> tab.
Access a map view of a selected node and its surrounding topology	Select the node of interest and use the <b>Actions</b> menu from the main toolbar to select either the Layer 2 or Layer 3 Neighbor View. See <a href="#">Using Table Views</a> for more information
View the statuses of interfaces on the node	If a node is not completely down, you might want to see which interfaces are down for the selected node. To do so, open the <b>Node</b> form and select the <b>Interfaces</b> tab.
The number of devices that are served by this node.	Select the node you want and access the Layer 2 or Layer 3 Neighbor View using the <b>Actions</b> menu.
View the status of all of the nodes that have been grouped together in a nodes group; for example, all of your important Cisco routers.	Your NNMi administrator can create Node Groups. These groups might contain only the nodes important to you. See <a href="#">Filter Information in a Table View</a> for more information.

### Related Topics:

[Using Table Views](#)

["Node Form" \(on page 28\)](#)

[Print Table Information](#)

## Interfaces View (Inventory)

**Tip:** See "[Interface Form](#)" (on page 60) for more details about the interface attributes that appear in this view's column headings.

The Interfaces view is useful for identifying the network interfaces managed by NNMi.

For each interface displayed in the view, you can identify the interface's overall status (for example, **Normal**, **Warning**, **Minor**, **Major**, **Critical**, or **Unknown**), its administrative (**AS**) and operational (**OS**) status, associated node Name value (**Hosted On Node**), the interface name, interface type, interface speed, input speed, output speed, the date the interface information was last changed, its description, the ifAlias value, and any notes included for the interface.

If you see several blank columns for an interface in a table view, the interface might be an interface on a

non-SNMP node or a Nortel private interface. Click here for more information.

For interfaces on non-SNMP nodes, note the following:

- The interface index (ifIndex) value is always set to **0** (zero).
- The interface type (ifType) is set to **Other**.
- The interface Name (ifName), if none is available, is set to **Pseudo Interface**.
- If the interface hosts an IP address, the interface Alias (ifAlias) is set to the IP address. Otherwise, the interface Alias (ifAlias) is set with information from neighboring SNMP devices.
- NNMi obtains the MAC address if the IP address can be resolved using ARP cache.

Note the following about **Pseudo** interfaces: NNMi attempts to obtain additional information using a variety of discovery protocols.

For Nortel SNMP interfaces, note the following:

- The ifIndex value is set according the Nortel private MIB.
- NNMi tries to collect the MAC address and interface name using Nortel's private MIBs.

Interface views are useful for quickly identifying items described in the following table.

#### Uses for Interfaces Views

Use	Description
View all network interfaces per node	Sort the view by <b>Hosted On Node</b> . This is the current value in NNMi's database for the Name attribute of the host device.
Determine the health of each of the managed interfaces	Sort the view by the <b>Status</b> attribute.  To view only those interfaces whose status is <b>Critical</b> , use the Critical Interfaces view provided by NNMi. See <a href="#">"Critical Interfaces View" (on page 120)</a> for more information.
Access a map view of the network interface and its surrounding topology.	Select the interface of interest and use the <b>Actions</b> menu to select either the Layer 2 or Layer 3 Neighbor view. See <a href="#">Using Table Views</a> for more information.
View the status of all of the interfaces that have been grouped together in a node or an interfaces group; for example, all of the interfaces on the important Cisco routers or all of the Voice-Over-IP interfaces within your network.	Your NNMi administrator can create nodes and interface groups. These groups might include only those nodes or interfaces important to you. Now you can filter the interfaces view by a node or an interface group. See <a href="#">Filtering a View by a Node or Interface Group</a> for more information.

#### Related Topics:

[Using Table Views](#)

["Interface Form" \(on page 60\)](#)

[Print Table Information](#)

## IP Addresses View (Inventory)



**Tip:** See ["IP Address Form" \(on page 73\)](#) for more information about the IP address attributes that appear in this view's column headings.

The IP Addresses view in the Inventory workspace is useful for identifying all of the IP addresses being managed by NNMi.

For each IP address displayed, you can identify its status, state, IP address, interface name (**In Interface**), associated node Name value (**Hosted On Node**), the subnet prefix (**In Subnet**) and prefix length (**PL**), and any notes included for the IP address.

The IP Address view is useful for quickly identifying items described in the following table.

### Uses for the IP Addresses View

Use	Description
View all IP addresses per node	Sort the view on <b>Hosted On Node</b> attribute.
View the addresses per interface	Sort the view on the Interface name ( <b>In Interface</b> ) attribute.
View the addresses per subnet	Sort the view on the subnet ( <b>In Subnet</b> ) attribute.
View the subnet information for a selected IP address	To access a subnet from this view: <ol style="list-style-type: none"> <li>1. Select the IP address of interest.</li> <li>2. Open the <b>IP Address</b> form</li> <li>3. Navigate to the <b>In Subnet</b> attribute. Click the  Lookup icon and select  Open to access the <b>IP Subnet</b> form.</li> </ol>
View the status of all of the addresses for the nodes that have been grouped together in a nodes group; for example, all of your important Cisco routers.	Your NNMi administrator can create node or interface groups. These groups might include only those nodes or interfaces important to you. Now you can filter the addresses view by a node or interface group. See <a href="#">Filtering a View by a Node or Interface Group</a> for more information.

### Related Topics:

[Use Table Views](#)

["IP Address Form" \(on page 73\)](#)

[Print Table Information](#)

## IP Subnets View (Inventory)

**Tip:** See ["IP Subnet Form" \(on page 113\)](#) for more details about the IP subnet attributes that appear in this view's column headings.

The IP Subnets view is useful for identifying all of the networks within your management domain.

For each IP subnet displayed, you can identify its name, the subnet prefix (**In Subnet**) and prefix length (**PL**), the date and time its status was last changed, and any notes included for the subnet.

The IP Subnets view is useful for quickly identifying items described in the following table.

### Uses for the Subnets View

Use	Description
Determine all nodes within a subnet	Use the Layer 3 Neighbor view to easily see the number of problem nodes within a subnet.
Browse for large and small subnets	Scan the <b>Name</b> column to view the list of available subnets.

You can identify empty subnets by opening the form for a selected subnet and viewing the IP addresses table.

#### Related Topics:

[Use Table Views](#)

["IP Subnet Form" \(on page 113\)](#)

[Print Table Information](#)

## VLANS View (Inventory)

A virtual local area network (VLAN) is a logical network within a physical network. The VLAN creates a reduced broadcast domain. Participating devices can physically reside in different segments of a LAN. The participating VLAN member devices behave "as if" they were all connected to one LAN.

Several VLANs can co-exist within a network. A device can participate in multiple VLANs. And a trunk port can participate in multiple VLANs.

There are several types of VLANs. NNMi supports switch port VLANs.

**Note:** NNMi does not currently support protocol-based VLANs and MAC-based VLANs.

#### To display the VLAN view:

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **VLANS** view.  
**Note:** NNMi ignores VLAN-1, but higher numbered VLANs are discovered.
3. Use the VLAN view to quickly identify all of the switch port VLANs configured in your network environment:

For each VLAN, the VLAN view displays the VLAN identification value, name, hostname of a representative node, IfName of a representative interface on the node, and member node count.

If your VLAN view contains two or more VLANs with the same name, those VLANs exist in separate broadcast domains.

#### Related Topics:

["VLAN Form" \(on page 86\)](#)

[Print Table Information](#)

## Layer 2 Connections View

**Tip:** See "[Layer 2 Connection Form](#)" (on page 106) for more details about the Layer 2 connection attributes that appear in this view's column headings.

The Layer 2 Connections view in the Inventory workspace is useful for identifying all of the connections being managed by NNMi. Sorting this view by Topology Source lets you easily identify all user added connections.

For each connection displayed in the view, you can identify the status, name, the data source or protocol (Topology Source) used to create the connection (for example **CDP** or **USER**), the date and time the connection was last modified, and any notes related to the connection.

### Related Topics

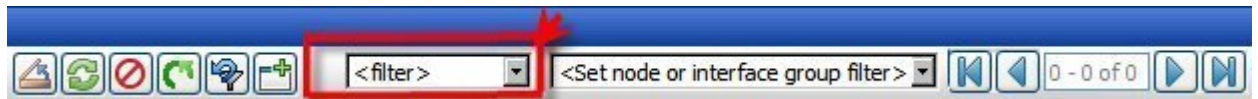
[Print Table Information](#)

## Nodes By Device Category View (Inventory)

**Tip:** See "[Node Form](#)" (on page 28) for more details about the node attributes that appear in this view's column headings.

The **Nodes by Device Category** view lets you filter your view by the device category value. Examples of device categories include **Firewall**, **Gateway**, **Hub**, and **Load Balancer**.

**Note:** By default, NNMi uses the first value in the Quick Filter list. If your view is empty, change the filter value. Here is an example of a Quick Filter list:



Use this view to monitor a specific category of devices. If your NNMi administrator set up Node Groups or Interface Groups to identify important elements of your environment, you can filter this view to show only devices of a certain category that are within a certain group of nodes. Using the device category and Node Group filters might be useful for troubleshooting purposes, so that you can take the same approach for devices in the same category.

**Note:** If you filter your view using additional filters, such as Node Groups, NNMi uses the AND operator to combine the filters you have selected. See [Filter a Table View](#) for more information.

For each node displayed, you can identify its overall status (for example, **Normal**, **Warning**, **Minor**, **Major**, **Critical**, or **Unknown**), name, hostname, management address, system location (the current value of the sysLocation MIB variable), device profile, date indicating the last time the node status was modified, and any notes included for the node.

### Related Topics

[Use Table Views](#)

[Filter a Table View](#)

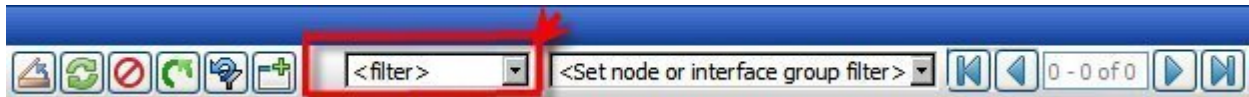
[Print Table Information](#)

## Interfaces by IfType View (Inventory)

**Tip:** See "[Interface Form](#)" (on page 60) for more details about the interface attributes that appear in this view's column headings.

The Interface by IfType view lets you filter your view by the Interface Type value. The list of interface types contains the industry standard known values for MIB II interface types. Examples of interface types include: **asynch**, **atm**, **bsc**, and **ces**.

**Note:** By default, NNMi uses the first value in the Quick Filter list. If your view is empty, change the filter value. Here is an example of a Quick Filter list:



Use this view to monitor a specific type of interfaces. If your NNMi administrator set up Node Groups or Interface Groups to identify important elements of your environment, you can filter this view to show only certain types of interfaces within a certain group of nodes. Using the type and Node Group filters might be useful for troubleshooting purposes.

**Note:** If you filter your view using additional filters, such as Node Groups, NNMi uses the AND operator to combine the filters you have selected. See [Filter a Table View](#) for more information.

For each interface displayed in the view, you can identify the interface's overall status (for example, **Normal**, **Warning**, **Minor**, **Major**, **Critical**, or **Unknown**), its administrative (**AS**) and operational (**OS**) status, associated node Name value (**Hosted On Node**), the interface name, interface speed, its description, its ifAlias value, the date the interface status was last modified, the name of the Layer 2 connection associated with the interface, and any notes that exist for the interface.

If you see several blank columns for an interface in a table view, the interface might be an interface on a non-SNMP node or a Nortel private interface. Click [here](#) for more information.

For interfaces on non-SNMP nodes, note the following:

- The interface index (ifIndex) value is always set to **0** (zero).
- The interface type (ifType) is set to **Other**.
- The interface Name (ifName), if none is available, is set to **Pseudo Interface**.
- If the interface hosts an IP address, the interface Alias (ifAlias) is set to the IP address. Otherwise, the interface Alias (ifAlias) is set with information from neighboring SNMP devices.
- NNMi obtains the MAC address if the IP address can be resolved using ARP cache.

Note the following about **Pseudo** interfaces: NNMi attempts to obtain additional information using a variety of discovery protocols.

For Nortel SNMP interfaces, note the following:

- The ifIndex value is set according the Nortel private MIB.
- NNMi tries to collect the MAC address and interface name using Nortel's private MIBs.

### Related Topics

[Using Table Views](#)

[Print Table Information](#)

## Custom Nodes View (Inventory)

**Tip:** See "[Node Form](#)" (on page 28) for more details about the node attributes that appear in this view's column headings.

The Custom Nodes view enables you to create a customized view of nodes. This view includes most of the attributes available for the node so that you can decide which are most important for you to display. See [Use Table Views](#) for more information about sorting, filtering, and hiding attributes within a view.

The Custom Nodes view includes the node's overall status (for example, **Normal**, **Warning**, **Minor**, **Major**, **Critical**, or **Unknown**), device category (**DC**), name, fully-qualified hostname (including the domain name, if available), management address, system location (the current value of the sysLocation MIB variable), device profile, date indicating the last time the node status was modified, any notes that exist for the node, its system name, system contact name, a system description, the management mode, the system object ID (MIB II sysObjectID), the name of its SNMP agent, its discovery state, whether the node is SNMP supported, the creation date, and the date the node was last modified.

See "[Nodes View \(Inventory\)](#)" (on page 16) for more information about ways to use a node view.

### Related Topics:

[Use Table Views](#)

[Print Table Information](#)

## Custom Interfaces View

**Tip:** See "[Interface Form](#)" (on page 60) for more details about the interface attributes that appear in this view's column headings.

The **Custom Interfaces** view lets you choose the columns of interface information, to better meet your needs. For example, you might want to filter the view to display only the interfaces related to a particular set of devices.

This view includes most of the attributes available for the incident so that you can decide which are most important for you to display. See [Use Table Views](#) for more information about sorting, filtering, and hiding attributes within a view.

For each interface displayed, you can view its state, its administrative and operational state, the associated hostname (Hosted On Node), its interface name, type, speed, description, the value of its alias, the date and time the status was last modified, the name of the Layer 2 connection associated with the interface, any notes related to the interface, its direct management mode, its node management mode, the physical address, the interface index, the creation date, and the date and time the interface was last modified.

If you see several blank columns for an interface in a table view, the interface might be an interface on a non-SNMP node or a Nortel private interface. [Click here](#) for more information.

For interfaces on non-SNMP nodes, note the following:

- The interface index (ifIndex) value is always set to **0** (zero).
- The interface type (ifType) is set to **Other**.
- The interface Name (ifName), if none is available, is set to **Pseudo Interface**.
- If the interface hosts an IP address, the interface Alias (ifAlias) is set to the IP address. Otherwise, the interface Alias (ifAlias) is set with information from neighboring SNMP devices.
- NNMi obtains the MAC address if the IP address can be resolved using ARP cache.

Note the following about **Pseudo** interfaces: NNMi attempts to obtain additional information using a variety of discovery protocols.

For Nortel SNMP interfaces, note the following:

- The ifIndex value is set according the Nortel private MIB.
- NNMi tries to collect the MAC address and interface name using Nortel's private MIBs.

See [Filter a Table View](#) for more information about how to filter information displayed in a table.

**Related Topics:**

[Use Table Views](#)

[Print Table Information](#)


## Router Redundancy Group View (NNMi Advanced)

**Tip:** See "[Router Redundancy Group Form \(NNMi Advanced\)](#)" (on page 79) for more details about the Router Redundancy Group attributes that appear in this view's column headings.;

Your network administrator might have set up groups of redundant routers to help ensure that information packets reach their intended destination. Use the Router Redundancy Group view to see all of the available groups of redundant routers in your network.

For each Router Redundancy Group displayed in the view, you can identify the Router Redundancy Group status, Router Redundancy Group name, the Router Redundancy Group protocol (for example, HSRP), and the date the Router Redundancy Group status was last modified.

**To see the incidents related to a Router Redundancy Group:**

1. Click the  Open icon that precedes the Router Redundancy Group of interest to open the form.
2. Navigate to the **Incidents** tab to see the incidents associated with the selected Router Redundancy Group.

**To view the members that belong to this group:**

Click the  Open icon that precedes the Router Redundancy Group of interest to open the form.

On the **Router Router Redundancy Members** tab, you should see a table view of the nodes and interfaces that belong to the selected Router Redundancy Group.

**Related Topics**

["Non-Normal Router Redundancy Group View \(NNMi Advanced\)" \(on page 123\)](#)

["Router Redundancy Group Form \(NNMi Advanced\)" \(on page 79\)](#)

[Print Table Information](#)

## Custom IP Addresses View (Inventory)

**Tip:** See "[IP Address Form](#)" (on page 73) for more details about the IP address attributes that appear in this view's column headings.

The Custom IP Addresses view displays most IP address attribute columns. Sort and filter this IP address view to meet your needs, if the out-of-the-box views provided by NNMi don't provide exactly what you want.



See [Use Table Views](#) for more information about sorting, filtering, and hiding attribute columns within a view.

For each address displayed in the view, you can identify the status, state, address, the name of the interface (**In Interface**), associated node Name value (**Hosted On Node**), the subnet in which the address is contained, the subnet prefix length (**PL**), the date the address status was last modified (**Status Last Modified**), any notes that exist for the IP address, its direct management mode, date the state of the address was last modified (**State Last Modified**), date the address was created, date the address was last modified.

See ["IP Address Form" \(on page 73\)](#) for more information about the IP address attributes.

### Related Topics

[Use Table Views](#)


[Print Table Information](#)

## Node Groups View (Inventory)

**Tip:** See ["Node Group Form" \(on page 88\)](#) for more details about the Node Group attributes that appear in this view's column headings

When checking your network inventory, you might be interested in only viewing information for a particular set of nodes. Your network administrator is able to group sets of nodes into node groups. An example node group could be all important Cisco routers, or all routers in a particular building. See [About Node and Interface Groups](#) for more information about how your administrator sets up node groups. See [Filter by Node or Interface Group](#) for more information about filtering views using node groups.

### To display the Node Groups view:

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **Node Groups** view.
3. To display the definition for a particular Node Group filter, click the  Open icon that precedes the Node Group of interest to open the form.

For each node group displayed in the view, you can identify the node group status, name, whether the node group appears in the filter list for node and interface views, whether the node group is available as a filter in the NNM iSPI Performance software, and any notes about the node group.

### Related Topics


[Print Table Information](#)

## Interface Group View (Inventory)

**Tip:** See ["Interface Group Form" \(on page 94\)](#) for more details about the Interface Group attributes that appear in this view's column headings.

When checking your network inventory, you might be interested in only viewing information for a particular set of interfaces. Your network administrator is able to group sets of interfaces into interface groups. See [About Node and Interface Groups](#) for more information about how your administrator sets up interface groups. See [Filter by Node or Interface Group](#) for more information about filtering views using interface groups.

### To display the Interface Group view:

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **Interface Group** view.
3. To display the definition for a particular Interface Group filter, click the  Open icon that precedes the Interface Group of interest to open the form.

For each interface group displayed in the view, you can identify the interface group name, whether the interface group appears in the filter list for interface views, whether the interface group is available as a filter in the NNM iSPI Performance software, and any notes about the interface group.

#### **Related Topics**

[Print Table Information](#)

## **Management Stations View (Inventory)**

Your NNMi administrator might configure NNMi so that you are able to view incidents that are being forwarded from a NNM management station (from either an NNM 6.x or 7.x management stations). If your NNMi administrator configured any NNM management stations, you are able to view this information using the **Inventory** workspace.

#### **To view attribute information for any NNM management stations that have been configured:**

From the **Workspaces** navigation pane, select **Inventory** → **Management Stations**.

The **Management Stations** view in the **Inventory** workspace is useful for identifying all of the NNM 6.x or 7.x management stations that might be forwarding incidents to your NNMi incident views, as well as launching directly to the NNM 6.x/7.x management station.

For each management station displayed, you can identify its name, the version of NNMi that is running on that machine (either 6.x or 7.x), the IP address for the machine, the OpenView Application Server (ovas) port number, the Web server port number, and a description for the management station that was provided by your NNMi administrator.

**Note:** If an NNM management station has been configured, you are also able to access the following 6.x or 7.x features from the NNMi **Actions** menu: Home Base, ovw, Launcher, and Alarms. See "[Accessing NNM 6.x and 7.x Features](#)" (on page 209) for more information.


#### **Related Topics**

[Print Table Information](#)

## Accessing Device Details

NNMi provides forms that help you easily view all details associated with a managed object, such as a node, SNMP agent, interface, address, subnet, or connection. NNMi also provides a Quick View that displays a small subset of information about an object.


### From a table view, to view all details associated with an object:

1. From the workspace navigation panel, select a workspace containing a view of the object of interest.
2. Select a view that contains the specific object (for example, **Inventory** → **Nodes**).
3. Click the  Open icon within the row representing the object.
4. The form displays, containing details of all information related to the object.
5. View or edit the details of the selected object:
  - ["Node Form" \(on page 28\)](#)["SNMP Agent Form" \(on page 50\)](#)
  - ["Interface Form" \(on page 60\)](#)
  - ["IP Address Form" \(on page 73\)](#)
  - ["Layer 2 Connection Form" \(on page 106\)](#)
  - ["IP Subnet Form" \(on page 113\)](#)
  - ["VLAN Form" \(on page 86\)](#)

**Tip:** A form is also available for incidents, see ["Incident Form" \(on page 134\)](#).



**Note:** NNMi also provides forms for SNMP Agent and Port objects. The SNMP Agent form is accessed from the Node form. The Port form is accessed from the VLAN form.

### From a map view, to view all details associated with an object:

1. Display a map using the **Troubleshooting** workspace, or the **Actions** → menu.
2. Select the object and click the  Open icon in the menu bar.
3. The form displays, containing details of all information related to the object.
4. View or edit the details of the selected object:
  - ["Node Form" \(on page 28\)](#)["SNMP Agent Form" \(on page 50\)](#)
  - ["Interface Form" \(on page 60\)](#)
  - ["IP Address Form" \(on page 73\)](#)
  - ["Layer 2 Connection Form" \(on page 106\)](#)
  - ["IP Subnet Form" \(on page 113\)](#)
  - ["VLAN Form" \(on page 86\)](#)

**Tip:** A form is also available for incidents, see ["Incident Form" \(on page 134\)](#).

### To access the Quick View for a selected object:

1. From the workspace navigation panel, select a workspace containing a view of the object of interest.
2. Select a table view that contains the specific object (for example, **Inventory** → **Nodes**).
3. In a table view, do one of the following:
  - Click the  Quick View icon within the row representing the object.
  - Using your mouse, hover over the  Quick View icon.
4. In a map view, using your mouse, hover over the object of interest.

The Quick View window displays, containing some of the details of the object.

**Related Topics:**

[Using Table Views](#)

[Using Map Views](#)

## Node Form

The Node form provides details about the selected node. It also provides details about the [interfaces](#), the [IP addresses](#), the [VLANs](#), the [ports](#), the [SNMP agent](#), the [device profile](#), and the [incidents](#) associated with this node.

If your role allows, you can use this form to modify the [Management Mode](#) for a node (for example to indicate it will be temporarily out of service) or add [notes](#) to communicate information about this node to your team.

**For information about each tab:**

### Basic Attributes

Attribute	Description
Name	<p>The name assigned to this device (according a strategy created by your NNMi administrator). The name might be a hostname determined by the hostname resolution strategy used in your environment (such as DNS), a MIB II sysName, or an address. Contact your NNMi administrator if you have questions.</p> <p>This name is used in table views and maps. This name cannot be modified in the Node form.</p>

Attribute	Description
Hostname	<p>The fully-qualified hostname for this device (according to any hostname resolution strategy currently in use in your network environment; for example, DNS).</p> <p><b>Note:</b> NNMi converts hostnames to all lowercase.</p> <p>If a device has multiple hostnames or no hostname, NNMi follows a set of rules to determine the hostname. Click here for details.</p> <ol style="list-style-type: none"> <li>1. If a hostname is available, it must resolve to a valid IP address. NNMi stores the fully-qualifiedhostname in the database as all lowercase characters.</li> <li>2. If more than one address is associated with a node, the <b>loopback address</b><sup>1</sup> is used with the following exceptions:                     <ul style="list-style-type: none"> <li>■ NNMi prefers loopback interfaces for management communication, where possible. However, NNMi automatically filters out addresses in the reserved loopback network range 127/24 (127.*.*).</li> <li>■ NNMi ignores any address that is virtual (HSRP/VRRP) or an <b>Anycast Rendezvous Point IP Address</b><sup>2</sup>.</li> </ul> </li> <li>3. If a node has multiple loopback addresses, NNMi uses the loopback address with the lowest number that resolves to a hostname (for example, 10.16.42.197 is a lower number than 10.16.197.42).</li> <li>4. If no loopback address resolves to a hostname and the device supports SNMP, NNMi uses the current value from the Management Address attribute on the Node form.</li> <li>5. If the device does not support SNMP, the IP address or DNS name found during the current rediscovery cycle is used as the hostname.</li> </ol> <p>This sequence is repeated during each rediscovery cycle. The hostname could change from cycle to cycle (for example, if an address did not respond to SNMP queries due to network problems or node reconfiguration).</p> <p>This name cannot be modified in the Node form.</p>
Management Address	<p>IP address NNMi uses to communicate with this node through SNMP. This is the IP address of the device's SNMP agent.</p>

<sup>1</sup>The address associated with the loopback interface. The loopback interface is a virtual interface on a device that provides a route for internal communication. Many vendors provide a specially configured loopback for management purposes. Exact details of how loopbacks are configured varies by vendor and model. See each device's documentation for details. NNMi identifies these loopback addresses by using IfType 24, softwareloopback from the IANA ifType-MIB.














<sup>2</sup>Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.





Attribute	Description
	<p><b>TIP:</b> The NNMi administrator can specify an address (Communication Configurations workspace, Specific Node Settings tab), or NNMi can dynamically select one.</p> <p>When NNMi determines the Management Address, NNMi handles cases where the SNMP agent supports multiple IP addresses by following a set of rules. Click here for details.</p> <ol style="list-style-type: none"><li>1. If the node has only one <b>loopback address</b><sup>1</sup>, that address is used with the following exceptions:<ul style="list-style-type: none"><li>■ NNMi prefers loopback interfaces for management communication, where possible. However, NNMi automatically filters out addresses in the reserved loopback network range 127/24 (127.*.*).</li><li>■ NNMi ignores any address that is virtual (HSRP/VRRP), an <b>Anycast Rendezvous Point IP Address</b><sup>2</sup>, or whose interface is administratively down.</li></ul></li><li>2. If an SNMP agent supports multiple loopback addresses, NNMi uses the loopback address with the lowest number to which this SNMP agent responds (for example, 10.16.42.197 is a lower number than 10.16.197.42).</li><li>3. If no loopback address is supported, NNMi uses the address that meets the following criteria:<ul style="list-style-type: none"><li>■ During initial discovery, NNMi uses the first address to which the associated SNMP agent responded. <b>Note:</b> The <i>first address</i> might be <i>either</i> a discovery seed address or an ARP cache address gathered in the path to this node.</li><li>■ During any other discovery cycle, NNMi uses the current Management Address value.</li></ul></li></ol> <p>For this sequence, if the SNMP agent does not respond to any of the above addresses, NNMi automatically repeats the sequence with SNMPv2c, SNMPv1, and SNMPv3 (according to the current NNMi Communication Configuration settings established by your NNMi administrator).</p> <p>This sequence is repeated during each configuration polling cycle. And the address could change over time (for example, if an address did not respond to SNMP queries due to network problems or node reconfiguration).</p> <p>If this field shows unexpected results:</p> <ul style="list-style-type: none"><li>● Use the <b>Actions</b> → <b>Configuration Poll</b> command to gather the most current information about this node.</li><li>● Check with your NNMi administrator. The NNMi administrator can configure a specific management address for this node in the Communication Configuration settings.</li></ul> <p><b>Note:</b> If the device does not support SNMP, this field is empty.</p>

---

<sup>1</sup>The address associated with the loopback interface. The loopback interface is a virtual interface on a device that provides a route for internal communication. Many vendors provide a specially configured loopback for management purposes. Exact details of how loopbacks are configured varies by vendor and model. See each device's documentation for details. NNMi identifies these loopback addresses by using IfType 24, softwareloopback from the IANA ifType-MIB.

<sup>2</sup>Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

Attribute	Description
Status	<p>Overall status for the current node. NNMi follows the ISO standard for status classification. See the <a href="#">"Node Form: Status Tab" (on page 48)</a> for more information. Possible values are:</p> <ul style="list-style-type: none"> <li> No Status</li> <li> Normal</li> <li> Disabled</li> <li> Unknown</li> <li> Warning</li> <li> Minor</li> <li> Major</li> <li> Critical</li> </ul> <p>The status of all IP addresses and the SNMP Agent associated with this node contribute to node status. For information about how the current status was determined, see the <a href="#">Conclusions tab</a>. Status reflects the most serious outstanding conclusion. See <a href="#">"Watch Status Colors" (on page 129)</a> for more information about possible status values.</p> <p><b>Note:</b> The icons are displayed only in table views.</p>
Node Management Mode	<p>Indicates whether the current node is being managed. This field also lets you specify whether a node is temporarily out of service. Possible values are:</p> <ul style="list-style-type: none"> <li> <b>Managed</b> – Indicates the node is managed by NNMi.</li> <li> <b>Not Managed</b> – Indicates the node is intentionally not managed. For example, the node might not be accessible because it is in a private network. NNMi does not update discovery information or monitor these nodes.</li> <li> <b>Out of Service</b> – Indicates a node is unavailable because it is out of service. NNMi does not update discovery information or monitor these nodes.</li> </ul> <p>This attribute is useful for notifying NNMi when a device has been temporarily out of service, or should never be managed.</p>
<b>SNMP Agent State Attributes</b>	
SNMP Supported	<p>Indicates whether the node responded to SNMP requests to determine whether the node has an SNMP agent.</p>
State	<p>Indicates whether the SNMP Agent assigned to this node is available and how NNMi is using SNMP to interact with this SNMP Agent. Possible values are:</p> <ul style="list-style-type: none"> <li> <b>Normal</b> – Indicates that the agent responded to an SNMP query.</li> <li> <b>Unresponsive</b> – Indicates that the SNMP agent did not respond to an SNMP query.</li> </ul> <p><b>Note:</b> State is determined by the State Poller Service. The current state contributes towards the status calculation for the node. See the <a href="#">Status tab</a> for more information.</p>

Attribute	Description
	mation.
State Last Modified	Indicates the date and time when the State value was last modified.
SNMP Agent	<p>Name used to identify the agent. By default, this name is the DNS resolved hostname for the node. The hostname is the fully-qualified hostname of the parent node (according to any hostname resolution strategy currently in use in your network environment; for example, DNS).</p> <p><b>Note:</b> NNMi converts hostnames to all lowercase.</p> <p>Click the  Lookup icon and select  Open to display the the <a href="#">"SNMP Agent Form" (on page 50)</a> for more information.</p>
<b>Discovery Attribute</b>	
Device Profile	<p>Name of the device profile that determines how devices of this type are managed and the icon and background shape displayed on maps.</p> <p>Click the  Lookup icon and select  Open to display the <a href="#">"Device Profile Form" (on page 56)</a> for more information.</p>
Discovery State	<p>Current discovery status for the node. Possible values are:</p> <p><b>Newly Created</b> – Indicates the node and its IP addresses are in the NNMi database, but further information needs to be collected before state and status are determined.</p> <p><b>Discovery Completed</b> – Indicates that all of the discovery information for the node has been collected.</p> <p><b>Rediscovery in Process</b> – Indicates discovery is updating information that has been collected for the node.</p>
Last Completed	Time of the last discovery cycle.
Notes	<p>Provided for network operators to use for any additional notes required to further explain the node. Information might include why the node is important, if applicable, or to what customer, department, or service the node is related. Additional information might include where the nodes is located, who is responsible for it, and its serial number. You might also track maintenance history using this attribute.</p> <p>Type a maximum of 1024 characters. Alpha-numeric, punctuation, spaces, and underline characters are allowed.</p> <p><b>Note:</b> You can sort your node table views based on this value. Therefore, you might want to include keywords for this attribute value.</p>


## Node Form: General Tab

The ["Node Form" \(on page 28\)](#) provides details about the selected node.

**For information about each tab:**



## SNMP Values


Attribute	Description
System Name	<p>The MIB II sysName value returned from the device's SNMP agent. This attribute is set by the device administrator.</p> <p>If sysName is part of the strategy used to populate the node Name attribute value, NNMi avoids populating the NNMi database with multiple devices having the same manufacturer's default name by following a set of rules. <a href="#">Click here for details.</a></p> <p>For each device type, NNMi has a Device Profile that includes a record of the manufacturer's default sysName. Other settings within the Device Profile can change the way NNMi determines sysName values.</p> <p>To view the Device Profile associated with this node, locate the <a href="#">Device Profile attribute</a> in the Basics section of the Node form, and click the  Lookup icon. Your NNMi administrator can make changes to a Device Profile, if necessary.</p>
System Contact	Optional MIB II sysContact value. This attribute is set by the device administrator. It usually includes the contact person for the managed node as well as information about how to contact this person.
System Description	Optional MIB II sysDescr value for the device description. This attribute is set by the device administrator.
System Object ID	MIB II sysObjectID value provided by the vendor. This value identifies the device vendor, type, and model. For example, all Cisco 6509 devices have the same system object ID.
System Location	Optional MIB sysLocation value for the physical location of the current node. For example, Building K, 3rd floor. This attribute is set by the device administrator.

## Node Form: IP Addresses Tab

The "[Node Form](#)" (on page 28) provides details about the selected node.

For information about each tab:

### IP Addresses Table


Attribute	Description
IP Addresses	<p>Table view of the IP addresses associated with the selected node. You can use this table to determine the status, state, address, interface, and subnet for each address associated with the selected node.</p> <p>Click the  Open icon to open the "<a href="#">IP Address Form</a>" (on page 73) and view more information about a specific address.</p>

## Node Form: Interfaces Tab

The "[Node Form](#)" (on page 28) provides details about the selected node.

For information about each tab:

## Interfaces Table


Attribute	Description
Interfaces	<p>Table view of all of the interfaces associated with the current node. You can use this table to determine the status, administrative state, operational state, name, type, interface speed, and Layer 2 connection for each interface associated with the selected node.</p> <p>Click the  Open icon to open the "<a href="#">Interface Form</a>" (on page 60) and view more information about a specific interface.</p>

## Node Form: VLAN Ports Tab

The "[Node Form](#)" (on page 28) provides details about the selected node.

For information about each tab:

### VLAN Ports Table










Attribute	Description
VLAN Ports	<p>Table view of all of the VLAN ports associated with the current node. Use this table to determine all port and VLAN combinations associated with this node.</p> <p>Click the  Open icon to open the Port form and view more information about a specific VLAN port.</p>

## VLAN Port Form

The VLAN Port form provides details about the VLAN port you selected on the Node or Interface form. The following table describes the fields included on the VLAN Port form.

### Basic Attributes

Attribute	Description
Port Name	The port name consists of <i>&lt;Card-number / Port-number&gt;</i> .
Member Node [Interface]	<p>NNMi selects a representative Member Node and Member Interface for the current VLAN. These members help to distinguish VLANs that use the same identification number.</p> <p>NNMi selects the Member Node using the following criteria:</p> <ul style="list-style-type: none"><li>• The node is a member of the VLAN.</li><li>• The node has the lexicographically ordered first node hostname.</li></ul> <p>NNMi selects the Member Interface using the following criteria:</p> <ul style="list-style-type: none"><li>• The interface must be on the Member Node.</li><li>• The interface is a member of the VLAN.</li><li>• The interface has the lexicographically ordered first interface name.</li></ul>
Member Node Count	Specifies the number of nodes that belong to the current VLAN.
VLAN	The identification value for the current VLAN. This value is taken directly from the MIB file provided by the Vendor.

Attribute	Description
	Click the  Lookup icon and select  Quick View or  Open to display more information about the VLAN.
Hosted on Node	Node on which the port resides. This is the current value in NNMi's database for the Name attribute of the host device. The value could be a DNS name, a MIB II sysName, or an address (depending on how your NNMi administrator configured the discovery process).  Click the  Lookup icon and select  Quick View or  Open to display more information about the node.
Associated Interface	The current value from the Name attribute on the Interface form. The most accurate interface name available to the initial discovery process: IF MIB ifName, ifAlias, or ifType+ifIndex values.  Click the  Lookup icon and select  Quick View or  Open to display more information about the interface.

**Related Topics:**

["Node Form" \(on page 28\)](#)


["VLAN Form" \(on page 86\)](#)

## Node Form: Ports Tab

The ["Node Form" \(on page 28\)](#) provides details about the selected node.

**For information about each tab:**

### Ports Table

Attribute	Description
Ports	Table view of all of the ports associated with the current node. You can use this table to determine the VLAN membership of each port associated with the selected node.  Click the  Open icon to open the <a href="#">"Port Form" (on page 87)</a> and view more information about a specific port.

## Node Form: Capabilities Tab

The Node Form: Capabilities Tab displays a table view of any capabilities added to the node object by NNMi or an external application. Capabilities enable NNMi and application programmers to provide more information about a node than is initially stored in the NNMi database. For example, NNMi Advanced uses the capability `com.hp.nnm.capability.rrp.hsrp` when a node is a member of an HSRP group.

**Note:** Because the values are generated by NNMi or an external application, Capability values cannot be modified.

**For information about each tab:**

### Capabilities Table

Attribute	Description
Capability	The name of the capability added to a node object by either NNMi or an external application.

Attribute	Description
	For more information, see: <ul style="list-style-type: none"> <li>• <a href="#">"Node Capability Form" (on page 38)</a></li> <li>• <a href="#">"Node Capabilities Provided by NNMi" (on page 36)</a></li> </ul>
Unique Key	The database identifier for the capability that either NNMi or an external application added to this node. <p><b>Note:</b> Capabilities added by NNMi use a Unique Key value that begins with the prefix: <code>com.hp.nnm.capability</code>. See <a href="#">"Node Capabilities Provided by NNMi" (on page 36)</a> for a description of the capabilities provided by NNMi that might appear on the Node Form: Capabilities Tab.</p>

## Node Capabilities Provided by NNMi

The Node Form: Capabilities Tab displays a table view of any capabilities added to the node object. Capabilities that begin with `com.hp.nnm.capability` represent capabilities that NNMi provides. External applications can also add node capabilities.

**Note:** NNMi also provides Capabilities on the Interface form **Capabilities** tab, additional abilities assigned to an interface by either NNMi or an external application. Capabilities enable NNMi and application programmers to provide more information about an interface than is initially stored in the NNMi database.

The following table includes the node capabilities NNMi provides to assist in determining node component health metrics. See ["Node Form: Component Health Tab" \(on page 40\)](#) for more information about health metrics.

Virtual Router Redundancy Protocol (VRRP) or Hot Standby Router Protocol (HSRP)

### NNMi Node Capabilities

Capability	Unique Key	Description
CHASSISMGREXT-MIB MIB	<code>com.hp.nnm.capability.metric.cme</code>	The node supports the indicated MIB.
CISCO-ENHANCED-BUFFER-MIB	<code>com.hp.nnm.capability.metric.ceb</code>	The node supports the indicated MIB.
CISCO-ENHANCED-MEMORY-POOL-MIB	<code>com.hp.nnm.capability.metric.cem</code>	The node supports the indicated MIB.
CISCO-ENVMON-MIB	<code>com.hp.nnm.capability.metric.cenv</code>	The node supports the indicated MIB.
Cisco Env Fan	<code>com.hp.com.capability.metric.cisco.env.fan</code>	The node supports CISCO-ENVMON-MIB.
Cisco Env Power	<code>com.hp.com.capability.metric.cisco.env.power</code>	The node supports CISCO-ENVMON-MIB.
Cisco Stack Fan	<code>com.hp.nnm.capability.metric.cisco.stack.fan</code>	The node supports CISCO-STACK-MIB.
Cisco Stack Power	<code>com.hp.nnm.capability.metric.cisco.stack.power</code>	The node supports

Capability	Unique Key	Description
		CISCO-STACK-MIB.
CISCO-MEMORY-POOL-MIB	com.hp.nnm.capability.metric.cmp	The node supports the indicated MIB.
CISCO-PROCESS-MIBv1	com.hp.nnm.capability.metric.cpm1	The node supports the indicated MIB.
CISCO-PROCESS-MIBv2	com.hp.nnm.capability.metric.cpm2	The node supports the indicated MIB.
CISCO-SYSTEM-EXT-MIB	com.hp.nnm.capability.metric.cse	The node supports the indicated MIB.
HOST-RESOURCES-MIB	com.hp.nnm.capability.metric.hr	The node supports the indicated MIB.
IP Forwarding (Layer 3)	com.hp.nnm.capability.node.ipforwarding	Value that indicates NNMi identified the selected node as a router that forwards Layer 3 data. NNMi evaluates SNMP MIB-II sysServices and other clues to determine this value and set the symbols in map views. The NNMi administrator can override this value using the Device Profile form, Force Device attribute (see " <a href="#">Device Profile Form</a> " (on page 56)).
LAN Switching (Layer 2)	com.hp.nnm.capability.node.lanswitching	Value that indicates NNMi identified the selected node as a switch for Layer 2 data. NNMi evaluates SNMP MIB-II sysServices and other clues to determine this value and set the symbols in map views. The NNMi administrator can override this value using the Device Profile form, Force Device attribute (see " <a href="#">Device Profile Form</a> " (on page 56)).
Nortel Passport Metrics	com.hp.nnm.capability.metric.rc	The node is a Nortel Passport device.

Capability	Unique Key	Description
Nortel BayStack Metrics	com.hp.nnm.capability.metric.s5	The node is a Nortel BayStack devices.
OLD-CISCO-BUFFER-MIB	com.hp.nnm.capability.metric.ocb	The node supports the indicated MIB.
OLD-CISCO-CPU-MIB	com.hp.nnm.capability.metric.occ	The node supports the indicated MIB.
OLD-CISCO-MEMORY-MI	com.hp.nnm.capability.metric.ocom	The node supports the indicated MIB.

### NNMi Advanced Additional Capabilities

Capability	Unique Key	Description
FDVRRP	com.hp.nnm.capability.rrp.fdvrrp	<i>NNMi Advanced.</i> The node is a member of a Foundry Virtual Router Redundancy Protocol (FDVRRP) group.
HPVRRP	com.hp.nnm.capability.rrp.hpvrrp	<i>NNMi Advanced.</i> The node is a member of an HP Virtual Router Redundancy Protocol (HPVRRP) group.
HSRP	com.hp.nnm.capability.rrp.hsrp	<i>NNMi Advanced.</i> The node is a member of an Hot Standby Router Protocol (HSRP) group.
RCVRRP	com.hp.nnm.capability.rrp.rcvrrp	<i>NNMi Advanced.</i> The node is a member of a Nortel Rapid City Virtual Router Redundancy Protocol (RCVRRP) group.
VRRP	com.hp.nnm.capability.rrp.vrrp	<i>NNMi Advanced.</i> The node is a member of a Virtual Router Redundancy Protocol (VRRP) group.

### Node Capability Form

This form describes a capability added to the node object by NNMi or an external application. Capabilities enable NNMi and application programmers to provide more information about a node than what is initially stored in the NNMi database. For example, NNMi Advanced uses the capability `com.hp.nnm-capability.rrp.hsrp` to identify when a node is a member of an HSRP group.

**Note:** Because the values are generated by NNMi or an external application, Capability values cannot be modified.

Each of the Capability attributes is described in the table below.

#### Basics Attributes

Attribute	Description
Capability	Label used to identify the Capability that was added to the node object. The Capability value is listed in the table on the Capabilities tab in a Node form. See <a href="#">"Node Form: Capabilities Tab" (on page 35)</a> .
Unique Key	Used as a unique identifier for the Capability. Any capability provided by NNMi begins with the prefix <code>com.hp.nnm.capability</code> .

Attribute	Description
-----------	-------------

**Note:** Capabilities added by NNMi use a Unique Key value that begins with the prefix: `com.hp.nnm.capability`. See ["Node Capabilities Provided by NNMi" \(on page 36\)](#) for a description of the capabilities provided by NNMi that might appear on the Node Form: Capabilities Tab.

## Node Form: Custom Attributes Tab

Custom Attributes enable an NNMi administrator to add information to the Node object. Custom Attributes can also be set by external applications that have been integrated with NNMi.

The Node Form: Custom Attributes Tab displays a table view of any Custom Attributes that have been added to the selected node. For example, your NNMi administrator might have added **Serial Number** as another attribute for the nodes in your network.

**Note:** If your role allows, you can edit a Custom Attribute. Only users assigned to the NNMi Administrator role can add a Custom Attribute.

For information about each tab:

### Custom Attributes Table

Attribute	Description
Name	Name used to identify the Custom Attribute.
Value	The actual value for the Custom Attribute for the selected node. For example, the value for the <b>Serial Number</b> attribute might be: <b>UHF536697J3</b>

## Node Custom Attributes Form

Custom Attributes enable an NNMi administrator to add information to a node object. For example, your NNMi administrator might have added **Serial Number** as another attribute for the nodes in your network. Custom Attributes can also be set by external applications that have been integrated with NNMi.

The Custom Attributes form displays the Name and Value for each of the Custom Attributes that were added to the node object. Each of these attributes is described in the table below.

### Basics Attributes


Attribute	Description
Name	Name used to identify the Custom Attribute. This name appears in the table view on the Custom Attributes tab in Node forms.
Value	Value assigned to the Custom Attribute for the selected node. For example, the value for the <b>Serial Number</b> attribute might be: <b>UHF536697J3</b> .

## Node Form: Node Groups Tab

The ["Node Form" \(on page 28\)](#) provides details about the selected node.

For information about each tab:

## Node Groups Table

Attribute	Description
Node Groups	Table view of all Node Groups to which this node belongs.  Click the  Open icon to view more information about a specific Node Group filter configuration.

## Node Form: Component Health Tab

The "[Node Form](#)" (on page 28) provides details about the selected node.

The Node Form: Component Health tab displays information about node health related to the following fault metrics:


- Fan
- Power Supply
- Temperature
- Voltage

(*NNM iSPI Performance for Metrics*) If the NNM iSPI Performance for Metrics software is installed and configured within your environment, the Node Form: Component Health tab also displays information about node health related to the following performance metrics:

- CPU utilization
- Memory utilization
- Buffer utilization
- Buffer miss rate
- Buffer failure rate

**For information about each tab:**

### Component Health Table

Attribute	Description
Component Health	Table view of the health metrics associated with the current node. You can use this table to determine the Status, Name, and Type for each health metric associated with the selected node.  Click the  Open icon to open the " <a href="#">Node Component Form</a> " (on page 40) and view more information about a specific metric and its monitored attributes.

## Node Component Form

This form describes the fault and performance metrics used to monitor node component health. NNMi obtains fault metrics from the node's MIB files. The NNMi administrator can set threshold values for each of the performance health metrics displayed.

Fault metrics include the following:

- Fan
- Power Supply











- Temperature
- Voltage

(*NNM iSPI Performance for Metrics*) The following performance metrics require an NNM iSPI Performance for Metrics license:

- CPU utilization
- Memory utilization
- Buffer utilization
- Buffer failures
- Buffer misses

For information about each tab:

### Basic Attributes

Attribute	Description
Status	<p>Overall status for the current node. NNMi follows the ISO standard for status classification. See the <a href="#">"Node Component Form: Status Tab " (on page 44)</a> for more information. Possible values are:</p> <ul style="list-style-type: none"> <li> No Status</li> <li> Normal</li> <li> Disabled</li> <li> Unknown</li> <li> Warning</li> <li> Minor</li> <li> Major</li> <li> Critical</li> </ul> <p>For information about how the current status was determined, see the <a href="#">Conclusions tab</a>. Status reflects the most serious outstanding conclusion. See <a href="#">"Watch Status Colors" (on page 129)</a> for more information about possible status values.</p> <p><b>Note:</b> The icons are displayed only in table views.</p>
Name	<p>Name of the node component whose health attribute is being measured, For example, NNMi measures fault metrics for Fan, Power Supply, Temperature, and Voltage node components.</p> <p>(<i>NNM iSPI Performance for Metrics</i>) If licensed and installed, NNM iSPI Performance for Metrics also measures performance metrics for CPU, memory, and buffer utilization, as well as for buffer failures and misses.</p> <p>When possible, NNMi obtains the Name value for the node component from the associated MIB file. The number of MIBs available and subsequently the number of health attributes that are measured for each node component vary. For example, if the node component is of type Buffer, up to five MIBs that contain information about the Buffer component are available (Small, Medium, Large, Big, and Huge). NNMi collects information from each MIB that is available and lists a node component Name value for each. For example, If all five MIBs are available, you see the following node components listed in the Component Health table: Small</p>


Attribute	Description
	<p>Buffers, Medium Buffers, Large Buffers, Big Buffers, and Huge Buffers.</p> <p><b>Note:</b> If the associated MIB file does not provide a name value, NNMi uses the value contained in the Type attribute.</p>
Type	<p>Identifies the aspect of node health that is being monitored. Possible values include:</p> <ul style="list-style-type: none"> <li>• Fan</li> <li>• Power Supply</li> <li>• Temperature</li> <li>• Voltage</li> </ul> <p>(<i>NNM iSPI Performance for Metrics</i>) The following performance types require an NNM iSPI Performance for Metrics license:</p> <ul style="list-style-type: none"> <li>• CPU utilization</li> <li>• Memory utilization</li> <li>• Buffer utilization</li> <li>• Buffer failures</li> <li>• Buffer misses</li> </ul>
Hosted On Node	<p>Node on which the health metric is being measured. This is the current value in NNMi's database for the Name attribute of the host device. The value could be a DNS name, a MIB II sysName, or an address (depending on how your NNMi administrator configured the discovery process).</p>

### Node Component Form: Health Attributes Tab

The "[Node Component Form](#)" (on page 40) provides details about the monitored attributes for the current node.

For information about each tab:

#### Attributes Table

Description
<p>Table view of the Name and State of each monitored attribute associated with the health metric for the selected node component. Use this view to determine the State of the monitored attributes for the selected node.</p> <p>Click the  Open icon to open the "<a href="#">Health Attribute Form</a>" (on page 42) and view more information about a specific attribute.</p>

#### Health Attribute Form

The Health Attribute form displays information about node component health related to the selected attribute .

Fault metrics are available for the following node components






- Fan
- Power Supply
- Temperature
- Voltage







NNMi obtains fault metric information from the associated MIB.

*(NNM iSPI Performance for Metrics)* If the NNM iSPI Performance for Metrics software is installed and configured within your environment, the Node Form: Component Health tab also displays information about node health related to the following performance metrics. The NNMi administrator sets the threshold for node components related to performance metrics:

- CPU utilization
- Memory utilization
- Buffer utilization
- Buffer miss rate
- Buffer failure rate

### Basics Attributes

Attribute	Description
Name	<p>Name used to identify the attribute being monitored.</p> <p>The number of health attributes available vary depending on the number of MIBs available for the current node component. See <a href="#">"Node Component Form" (on page 40)</a> for more information.</p> <p>The Name of each health attribute identifies the attribute being measured as well as the type of MIB used to gather this information. For example, when monitoring CPU utilization, NNMi uses values measured for 1-minute, 5-minute, and 5-second intervals. Each of these values might be available from an old, standard, or most recent (revised) MIB file. The following example health attribute names indicate the CPU measurement interval as well as the fact that the information was collected from the most recent (revised) MIB:</p> <ul style="list-style-type: none"> <li>• CPU Revised 1 Minute</li> <li>• CPU Revised 5 Minute</li> <li>• CPU Revised 5 Second</li> </ul>
State	<p>Normalized value used to indicate the State of the health attribute on the selected node. Possible values are listed below.</p> <p><b>Note:</b> The NNMi State Poller interprets and normalizes the State value returned for the monitored attribute to handle the differences between vendor-specific nodes.</p> <ul style="list-style-type: none"> <li> <b>Normal</b> - Indicates there are no known problems related to the associated object.</li> <li> <b>Warning</b> - Indicates there may or may not be a problem related to the associated object.</li> <li> <b>Minor</b> - Indicates NNMi has detected problems related to the associated object that require further investigation.</li> <li> <b>Major</b> - Indicates NNMi detected problems that could precede a critical situation.</li> <li> <b>Critical</b> - Indicates NNMi detected problems that require immediate attention.</li> </ul>

Attribute	Description
	<p>One of following States is returned when the monitored attribute is not polled or when the State data returned for the monitored attribute is either unavailable or in error:</p> <p> <b>Not Polled</b> - Indicates that this health attribute is intentionally not polled, based on current Monitoring Configuration settings, current Communication Configuration settings, or because the parent Node is set to Not Managed or Out of Service</p> <p> <b>No Polling Policy</b> - No polling policy exists for this monitored attribute.</p> <p> <b>Unavailable</b> - Unable to determine the State. For example, the value returned might be outside the range of possible values.</p> <p><b>Note:</b> State is determined by the State Poller Service. The current state contributes towards the status calculation for the node. See the <a href="#">Status tab</a> for more information.</p> <p>(<i>NNMi SPI Performance for Metrics</i>) Additional States for performance metrics include the following (<b>Warning</b> and <b>Critical</b> states are not used for performance metrics):</p> <p> <b>High</b> - The High threshold was crossed.</p> <p> <b>Low</b> - The Low threshold was crossed.</p> <p> <b>None</b> - The threshold value returned is zero.</p>


### Node Component Form: Incidents Tab

**Tip:** See "[Incident Form](#)" ([on page 134](#)) for more details about the incident attributes that appear in the incident view's column headings.

The "[Node Component Form](#)" ([on page 40](#)) provides details about the monitored attributes for the selected node.

**For information about each tab:**

#### Incidents Table

Description
<p>Table view of the incidents associated with the selected monitored attribute. These incidents are sorted by creation time so that you can view the incidents in chronological order. Use this view to determine which incidents are still open for the monitored attribute.</p> <p>Click the  Open icon to open the "<a href="#">Incident Form</a>" (<a href="#">on page 134</a>) and view more information about a specific incident.</p>









### Node Component Form: Status Tab

The "[Node Component Form](#)" ([on page 40](#)) provides details about the selected health metric for the current node.

**For information about each tab:**

#### Overall Status

Attribute	Description
Status	Overall status for the current node. NNMi follows the ISO standard for status classification.

Attribute	Description
	<p>Possible values are:</p> <ul style="list-style-type: none"> <li> No Status</li> <li> Normal</li> <li> Disabled</li> <li> Unknown</li> <li> Warning</li> <li> Minor</li> <li> Major</li> <li> Critical</li> </ul> <p><b>Note:</b> Your NNMi administrator might have disabled polling of Node Component Health using the Monitoring Configuration workspace.</p> <p>The status of the health metric associated with this node contributes to the node's overall status. For information about how the current status was determined, see the <a href="#">"Node Component Form: Conclusions Tab" (on page 45)</a>. Status reflects the most serious outstanding conclusion. See <a href="#">"Watch Status Colors" (on page 129)</a> for more information about possible status values.</p> <p><b>Note:</b> The icons are displayed only in table views.</p>
Status Last Modified	Date and time indicating when the status was last set.


### Node Component Form: Conclusions Tab

The ["Node Component Form" \(on page 40\)](#) provides details about the selected health metric for the current node.

**For information about each tab:**

#### Outstanding Status Conclusions Table

Attribute	Description
Status Conclusions	<p>The dynamically generated list of summary statuses of the monitored attribute at points in time that contributed to the current overall status of the selected node. Status is set by the Causal Engine.</p> <p>Each conclusion listed is outstanding and contributes to the current overall status.</p> <p>This view is useful for obtaining a quick summary of the problem description for the current monitored attribute that led up to the node's most current status.</p> <p>The status value is correlated based on the most critical conclusions.</p> <p>To see more information about a specific conclusion:</p>

Attribute	Description
	<ol style="list-style-type: none"> <li>1. Select the conclusion of interest by checking the <input checked="" type="checkbox"/> selection box that precedes the object information.</li> <li>2. Click the  Open icon to view more information about a specific conclusion.</li> </ol>

## Node Form: Diagnostics Tab (NNM iSPI NET)

(NNM iSPI Network Engineering Toolset) The "[Node Form](#)" (on page 28) provides details about the selected node.

When you access the Node Form: Diagnostics Tab, you can view the history of all the NNM iSPI Network Engineering Toolset Diagnostic reports that have been run for this Node. Diagnostics are sets of automated commands specific to one or more device types, including Cisco routers and switches, Cisco switch/routers, and Nortel switches.

To generate a new instance of these Diagnostics reports, click **Actions** → **Run Diagnostics**.

For information about each tab:

### Diagnostics Table

Attribute	Description
Start Time	Date and time NNM iSPI NET created this instance of the Diagnostics report. NNM iSPI NET uses the locale of the client and the date and time from the NNMi management server.
Definition	The name of the NNM iSPI NET Diagnostics report definition.
Status	<p>The current status of this NNM iSPI NET Diagnostics report. Possible values include:</p> <p><b>New</b> - The Diagnostic is in the queue, but is not yet running</p> <p><b>In Progress</b> - The Diagnostic has been submitted and is not finished running</p> <p><b>Completed</b> - The Diagnostic has finished running</p> <p><b>Not Submitted</b> - An error condition prevented the Diagnostic from being submitted</p> <p><b>Timed Out</b> - NNMi was unable to submit or run the Diagnostic due to a time out error. The time out limit for submitting a Diagnostic is one hour. The time out limit for running a Diagnostic is four hours.</p> <p>Example error conditions include the following:</p> <ul style="list-style-type: none"> <li>• The number of Diagnostics in the queue might prevent NNMi from submitting the Diagnostic.</li> <li>• A configuration error, such as an incorrect user name or password, might prevent NNMi from accessing the required Operations Orchestration server.</li> </ul> <p>Contact your NNMi administrator for Diagnostic log file information.</p>
Report	<p>Click this link to open the actual report.</p> <p><b>Note:</b> You might be prompted to provide a user name and password to access the Operations Orchestration software. See the <i>NNM iSPI NET Planning and Installation Guide</i> for more information.</p>
Last Update	Date and time NNM iSPI NET last updated this instance of the Diagnostics report. NNM iSPI NET uses the locale of the client and the date and time from the NNMi management server.

Attribute	Description
Time	

### Node Diagnostic Results Form (Flow Run Result) (NNM iSPI NET)

NNM iSPI Network Engineering Toolset automatically prepares diagnostic reports about the source node when certain incidents are generated and when using **Actions** → **Run Diagnostics**. This form shows details about the currently selected diagnostic report instance.

**Note:** Because the values on this form are generated by NNM iSPI NET, these attribute values cannot be modified.

See "[Node Form: Diagnostics Tab \(NNM iSPI NET\)](#)" (on page 46) for more information.

#### Diagnostic Results Details

Attribute	Description
Start Time	The time that NNM iSPI NET created the selected diagnostic report instance.
Definition	The name of the flow as defined in NNM iSPI NET.
Status	<p>The current status of this NNM iSPI NET Diagnostics report. Possible values include:</p> <p><b>New</b> - The Diagnostic is in the queue, but is not yet running</p> <p><b>In Progress</b> - The Diagnostic has been submitted and is not finished running</p> <p><b>Completed</b> - The Diagnostic has finished running</p> <p><b>Not Submitted</b> - An error condition prevented the Diagnostic from being submitted</p> <p><b>Timed Out</b> - NNMi was unable to submit or run the Diagnostic due to a time out error. The time out limit for submitting a Diagnostic is one hour. The time out limit for running a Diagnostic is four hours.</p> <p>Example error conditions include the following:</p> <ul style="list-style-type: none"> <li>• The number of Diagnostics in the queue might prevent NNMI from submitting the Diagnostic.</li> <li>• A configuration error, such as an incorrect user name or password, might prevent NNMI from accessing the required Operations Orchestration server.</li> </ul> <p>Contact your NNMi administrator for Diagnostic log file information.</p>
Report	NNM iSPI NET uses this text string to display the selected instance of the diagnostics report in a browser window.
Lifecycle State	<p>The Incident's Lifecycle State that determines when this Diagnostic runs. Possible values include:</p> <ul style="list-style-type: none"> <li>• Registered</li> <li>• In Progress</li> <li>• Completed</li> <li>• Closed</li> </ul> <p>See <a href="#">About the Incident Lifecycle</a> for more information about Lifecycle State.</p>

Attribute	Description
	When the Incident is set to this Lifecycle State, the selected Diagnostics (Flow Definitions) is automatically run on each applicable Source Node in the specified Node Group.
Last Update Time	Date and time NNM iSPI NET last updated this instance of the Diagnostics report. NNM iSPI NET uses the locale of the client and the date and time from the NNMi management server.


## Node Form: Incidents Tab

**Tip:** See ["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in the incident table view's column headings.

The ["Node Form" \(on page 28\)](#) provides details about the selected node.

**For information about each tab:**

### Incidents Table









Description
Table view of the incidents associated with the selected node. These incidents are sorted by creation time so that you can view the incidents in chronological order. Use this view to determine which incidents are still open for the selected node.
Click the  Open icon to open the <a href="#">"Incident Form" (on page 134)</a> and view more information about a specific incident.

## Node Form: Status Tab

The ["Node Form" \(on page 28\)](#) provides details about the selected node.

**For information about each tab:**


### Overall Status

Attribute	Description
Status	<p>Overall status for the current node. NNMi follows the ISO standard for status classification. Possible values are:</p> <ul style="list-style-type: none"> <li> No Status</li> <li> Normal</li> <li> Disabled</li> <li> Unknown</li> <li> Warning</li> <li> Minor</li> <li> Major</li> <li> Critical</li> </ul> <p>The status of all IP addresses and the SNMP Agent associated with this node, and well as</p>



Attribute	Description
	<p>interface health contribute to node status. For information about how the current status was determined, see the <a href="#">"Node Form: Conclusions Tab" (on page 49)</a>. Status reflects the most serious outstanding conclusion. See <a href="#">"Watch Status Colors" (on page 129)</a> for more information about possible status values.</p> <p>Your NNMi administrator might configure Custom Poller so that the Status of a Custom Node Collection effects the topology node's Status. Click here to view the effect of a Custom Node Collection's Status on the topology node's Status. See <a href="#">About Custom Poller</a> for more information.</p> <p>The effect of a Custom Node Collection's Status on the topology node's Status is determined as follows:</p> <ul style="list-style-type: none"> <li>• If at least one Custom Collection Node's Status is Critical, the topology node Conclusion Status is Critical.</li> <li>• If at least one Custom Collection Node's Status is Major, but none are Critical, the topology node Conclusion Status is Major.</li> <li>• If at least one Custom Collection Node's Status is Minor, but none are Critical or Major, the topology node Conclusion Status is Minor.</li> <li>• At least one Custom Collection Node's Status is Warning, but none are Critical, Major, or Minor, the topology node Conclusion Status is Warning.</li> <li>• If the Status of all Custom Collection Nodes are Normal, the topology node Conclusion Status is Normal.</li> </ul> <p><b>Note:</b> The icons are displayed only in table views.</p>
Status Last Modified	Date and time indicating when the status was last set.

### Status History Table

Attribute	Description
Status History	<p>List of up to the last 30 changes in status for the selected node. This view is useful for obtaining a summary of the node status so that you can better determine any patterns in node behavior and activity.</p> <p>Click the  Open icon to view more information about a specific status.</p>


### Node Form: Conclusions Tab

The ["Node Form" \(on page 28\)](#) provides details about the selected node.

**For information about each tab:**

### Outstanding Status Conclusions Table

Attribute	Description
Status Conclusions	The dynamically generated list of summary statuses of the node at points in time that contributed to the current overall status of the selected node. Status is set by the Causal

Attribute	Description
	Engine. Each conclusion listed is still outstanding and applies to the current overall status. This view is useful for obtaining a quick summary of the status and problem description for the current node's interfaces that led up to the node's most current status. Examples of conclusions that might appear together are listed below: <ul style="list-style-type: none"><li>• SNMP Agent Not Responding</li><li>• Interface Down</li><li>• Address Down</li></ul> The status value is correlated based on the most critical conclusions. Click the  Open icon to view more information about a specific conclusion.

## Node Form: Registration Tab

The "[Node Form](#)" (on page 28) provides details about the selected node.

**For information about each tab:**

### Registration

Attribute	Description
Created	Date and time the selected object instance was created. NNM uses the locale of the client and the date and time from the NNMi management server.
Last Modified	Date the selected object instance was last modified. NNM uses the locale of the client and the date and time from the NNMi management server.

## SNMP Agent Form

The SNMP Agent form provides details about the SNMP Agent assigned to the currently selected node. This form is useful when you want to view more details about the SNMP Agent, including the agent's status. You can also use the form to determine all of the attributes in the NNMi database associated with the SNMP Agent.

**For information about each tab:**

## Basic Attributes

Attribute	Description
Name	<p>Name used to identify the agent. By default, this name is the DNS resolved hostname for the node. The hostname is the fully-qualified hostname of the parent node (according to any hostname resolution strategy currently in use in your network environment; for example, DNS).</p> <p><b>Note:</b> NNMi converts hostnames to all lowercase.</p> <p>If a device has multiple hostnames or no hostname, NNMi follows a set of rules to determine the hostname. Click here for details.</p> <ol style="list-style-type: none"><li>1. If a hostname is available, it must resolve to a valid IP address. NNMi stores the fully-qualifiedhostname in the database as all lowercase characters.</li><li>2. If more than one address is associated with a node, the <b>loopback address</b><sup>1</sup> is used with the following exceptions:<ul style="list-style-type: none"><li>■ NNMi prefers loopback interfaces for management communication, where possible. However, NNMi automatically filters out addresses in the reserved loopback network range 127/24 (127.*.*).</li><li>■ NNMi ignores any address that is virtual (HSRP/VRRP) or an <b>Anycast Rendezvous Point IP Address</b><sup>2</sup>.</li></ul></li><li>3. If a node has multiple loopback addresses, NNMi uses the loopback address with the lowest number that resolves to a hostname (for example, 10.16.42.197 is a lower number than 10.16.197.42).</li><li>4. If no loopback address resolves to a hostname and the device supports SNMP, NNMi uses the current value from the Management Address attribute on the Node form.</li><li>5. If the device does not support SNMP, the IP address or DNS name found during the current rediscovery cycle is used as the hostname.</li></ol> <p>This sequence is repeated during each rediscovery cycle. The hostname could change from cycle to cycle (for example, if an address did not respond to SNMP queries due to network problems or node reconfiguration).</p> <p>This name cannot be modified in the Node form.</p>

---

<sup>1</sup>The address associated with the loopback interface. The loopback interface is a virtual interface on a device that provides a route for internal communication. Many vendors provide a specially configured loopback for management purposes. Exact details of how loopbacks are configured varies by vendor and model. See each device's documentation for details. NNMi identifies these loopback addresses by using IfType 24, softwareloopback from the IANA ifType-MIB.

<sup>2</sup>Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.






Attribute	Description
Management Address	<p>IP address NNMi uses to communicate with this SNMP agent.</p> <p><b>TIP:</b> The NNMi administrator can specify an address (Communication Configurations workspace, Specific Node settings tab), or NNMi can dynamically select one.</p> <p>When NNMi determines the Management Address, NNMi handles cases where the SNMP agent supports multiple IP addresses by following a set of rules. Click here for details.</p> <ol style="list-style-type: none"> <li>If the node has only one <b>loopback address</b><sup>1</sup>, that address is used with the following exceptions:                             <ul style="list-style-type: none"> <li>NNMi prefers loopback interfaces for management communication, where possible. However, NNMi automatically filters out addresses in the reserved loopback network range 127/24 (127.*.*).</li> <li>NNMi ignores any address that is virtual (HSRP/VRRP), an <b>Anycast Rendezvous Point IP Address</b><sup>2</sup>, or whose interface is administratively down.</li> </ul> </li> <li>If an SNMP agent supports multiple loopback addresses, NNMi uses the loopback address with the lowest number to which this SNMP agent responds (for example, 10.16.42.197 is a lower number than 10.16.197.42).</li> <li>If no loopback address is supported, NNMi uses the address that meets the following criteria:                             <ul style="list-style-type: none"> <li>During initial discovery, NNMi uses the first address to which the associated SNMP agent responded.                                     <p><b>Note:</b> The <i>first address</i> might be <i>either</i> a discovery seed address or an ARP cache address gathered in the path to this node.</p> </li> <li>During any other discovery cycle, NNMi uses the current Management Address value.</li> </ul> </li> </ol> <p>For this sequence, if the SNMP agent does not respond to any of the above addresses, NNMi automatically repeats the sequence with SNMPv2c, SNMPv1, and SNMPv3 (according to the current NNMi Communication Configuration settings established by your NNMi administrator).</p> <p>This sequence is repeated during each configuration polling cycle. And the address could change over time (for example, if an address did not respond to SNMP queries due to network problems or node reconfiguration).</p>
Protocol Version	Version of the SNMP protocol in use. NNMi supports versions SNMPv1, SNMPv2c, and SNMPv3.
Read Community String	<p>Community string value that was discovered for the selected SNMP agent.</p> <p><b>Note:</b> The community string is an SNMPv1 or SNMPv2c password. The actual community string is only visible if you are assigned to the Administrator role.</p>




<sup>1</sup>The address associated with the loopback interface. The loopback interface is a virtual interface on a device that provides a route for internal communication. Many vendors provide a specially configured loopback for management purposes. Exact details of how loopbacks are configured varies by vendor and model. See each device's documentation for details. NNMi identifies these loopback addresses by using IfType 24, softwareloopback from the IANA ifType-MIB.

<sup>2</sup>Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

Attribute	Description
UDP Port	User Datagram Protocol port configuration for this SNMP agent.  Default 161. Port NNMi is instructed to use when contacting this SNMP agent to collect SNMP data. Both the Discovery Process and the State Poller Service use this setting.
SNMP Proxy Address	<i>Prerequisite:</i> The NNMi administrator must specify one or more SNMP Proxy Servers in the NNMi Communication Configuration settings.  The IP address of the server that is acting as the SNMP Proxy Server for this SNMP agent. Your NNMi administrator might have set up one or more SNMP Proxy Servers to enable communication with nodes that otherwise might be unreachable. For example, when a node to be managed is behind a firewall. The SNMP Proxy Server allows NNMi to manage these nodes in the same way as nodes that provide SNMP access directly.
SNMP Proxy Port	<i>Prerequisite:</i> The NNMi administrator must specify one or more SNMP Proxy Servers in the NNMi Communication Configuration settings.  The port number on the server that is acting as the SNMP Proxy Server for this SNMP Agent. See SNMP Proxy Address (previous attribute) for more information.
SNMP Time-out	(Seconds:Milliseconds) Time that NNMi waits for a response to an SNMP query before reissuing the request.
SNMP Retries	Maximum number of retries that NNMi issues for an SNMP query before determining the query result to be "unresponsive". Zero means no retries.

#### SNMP Agent State Attributes

State	<p>Indicates whether the SNMP agent is available and how NNMi is using SNMP to interact with this SNMP agent. Possible values are:</p> <ul style="list-style-type: none"> <li> <b>Normal</b> – Indicates that the agent is being polled and is responding to SNMP queries.</li> <li> <b>Unresponsive</b> – Indicates that the agent is being polled, but did not respond to SNMP queries.</li> <li> <b>Unset</b> – Indicates that discovery is gathering initial information. The State of the SNMP agent remains <b>Unset</b> until the first configured polling cycle completes.</li> <li> <b>Not Polled</b> – Indicates that this SNMP Agent's address is intentionally not polled, based on current Monitoring Configuration settings, current Communication Configuration settings, or because the parent Node is set to Not Managed or Out of Service.</li> <li> <b>No Polling Policy</b> – Indicates that this SNMP Agent's address is not included in any Monitoring Configuration settings, and therefore not polled.</li> </ul> <p><b>Note:</b> NNMi's State Poller sets this state. The current state contributes towards the status calculation for the agent. See <a href="#">"SNMP Agent Form: Status Tab" (on page 54)</a> for more information.</p>
State Last Modified	Indicates the date and time when the State value was last modified.
Hosted On Node	Node on which the SNMP Agent resides. This is the current value in NNMi's database for










Attribute	Description
	<p>the Name attribute of the host device. The value could be a DNS name, a MIB II sysName, or an address (depending on how your NNMi administrator configured the discovery process).</p> <p>Click the  Lookup icon and select  Quick View or  Open to display more information about the node.</p>

## SNMP Agent Form: Status Tab

The "[SNMP Agent Form](#)" (on page 50) provides details about the SNMP Agent of the selected node or interface.

For information about each tab:

### Status


Attribute	Description
Status	<p>Overall status for the current SNMP agent. NNMi follows the ISO standard for status classification. Possible values are:</p> <ul style="list-style-type: none"> <li> No Status</li> <li> Normal</li> <li> Disabled</li> <li> Unknown</li> <li> Warning</li> <li> Minor</li> <li> Major</li> <li> Critical</li> </ul> <p>For information about how the current status was determined, see "<a href="#">SNMP Agent Form: Conclusions Tab</a>" (on page 54). Status reflects the most serious outstanding conclusion.</p>
Status Last Modified	Date and time indicating when the status was last set.
Status History	<p>List of the changes in the status for the SNMP agent.</p> <p>Click the  Open icon to view more information about a specific status.</p>

## SNMP Agent Form: Conclusions Tab

The "[SNMP Agent Form](#)" (on page 50) provides details about the SNMP Agent of the selected node or interface.

For information about each tab:

## Conclusions Table


Attribute	Description
Outstanding Status Conclusion	<p>The dynamically generated list of summary statuses for the SNMP agent at points in time that contributed to the current overall status of the selected SNMP agent. Status is set by the Causal Engine.</p> <p>Each conclusion listed is still outstanding and applies to the current overall status.</p> <p>This view is useful for obtaining a quick summary of how the status of interfaces on the node contributes to the current status of the node.</p> <p>Examples of conclusions that might appear together are listed below:</p> <ul style="list-style-type: none"> <li>• SNMP Agent Not Responding</li> <li>• Interface Down</li> <li>• Some Unresponsive Addresses In Node</li> <li>• Address Not Responding</li> </ul> <p>The status value is correlated based on the most critical conclusions.</p> <p>Click the  Open icon to view more information about a specific conclusion.</p>

## SNMP Agent Form: Incidents Tab

The "[SNMP Agent Form](#)" (on page 50) provides details about the SNMP Agent of the selected node or interface.

For information about each tab:

### Incidents Table

Attribute	Description
Associated Incidents	<p>Table view of the incidents associated with the selected SNMP agent. These incidents are sorted by creation time so that you can view the incidents in chronological order. Use this view to determine which incidents are still open for the selected SNMP agent.</p> <p>Click the  Open icon to open the "<a href="#">Incident Form</a>" (on page 134) and view more information about a specific incident.</p>

## SNMP Agent Form: Registration Tab

The "[SNMP Agent Form](#)" (on page 50) provides details about the SNMP Agent of the selected node or interface.

For information about each tab:

### Registration





Attribute	Description
Created	Date and time the selected object instance was created. NNM uses the locale of the client and the date and time from the NNMi management server.
Last Modified	Date the selected object instance was last modified. NNM uses the locale of the client and the date and time from the NNMi management server.

## Device Profile Form

According to industry standards (RFC 1213, MIB II), each combination of vendor, device type, and model number is assigned a unique SNMP system object ID (sysObjectID). For example, all Cisco 6500 series switches have the same sysObjectID prefix: .1.3.6.1.4.1.9.\* See the [Basic Attributes](#).

NNMi uses the [Advanced Settings](#) to make decisions about how devices are discovered and depicted on the NNMi maps.

### Basic Attributes

Attribute	Description
Device Model	Device model name or number designator, determined by the vendor.
SNMP Object ID	MIB II sysObjectID number issued for this device type. These numbers are unique across all vendors.
Description	The description, based on information from the MIB II sysDescr string provided by the vendor.  Maximum length 255 characters. Alpha-numeric, punctuation, spaces, and underline characters allowed.
Device Family	Device family name provided by the vendor; for example Cisco Catalyst 6500 Series Switches or HP AdvanceStack Routers.  Click the  Lookup icon to access the <a href="#">"Device Family Form" (on page 58)</a> for more details.
Device Vendor	Name of the vendor that manufactures the device.  Click the  Lookup icon to access the <a href="#">"Device Vendor Form" (on page 58)</a> for more details.
Device Category	The value of this attribute determines which background shape NNMi uses for the map icon representing devices of this type. See <a href="#">"About Map Symbols"</a> for more information about the possible values.  Click the  Lookup icon to access the <a href="#">"Device Category Form" (on page 59)</a> for more details.
OUI	Organizationally unique identifier. The first three octets of the MAC address for the device that identify the device's vendor.
Author	Indicates who created the device profile. All profiles provided by NNMi have the value "HP Network Node Manager".  Click the  Lookup icon to access the <a href="#">"Device Profile Author Form" (on page 59)</a> for more details.

### Advanced Settings Tab

Attribute	Description
<b>Use of SNMP SysName for Node Name Resolution</b>	



Attribute	Description
Never Use sysName	<p>If <input checked="" type="checkbox"/> enabled, Spiral Discovery does not allow a MIB II sysName value for the Name attribute for discovered Nodes of this type. If sysName is part of the current node Name strategy, NNMi uses the next designated node Name choice in the strategy established by your NNMi administrator.</p> <p>If <input type="checkbox"/> disabled, MIB II sysName can potentially be used as the Name attribute value for nodes of this type.</p>
Do not Use sysName Starting With	<p>The vendor's default sysName text string, from MIB II sysName.</p> <p>If the SNMP agent responds to a sysName request with a value that matches or starts with the entry in this field (case-sensitive), Spiral Discovery ignores the sysName and considers sysName to be unset. As a result, NNMi instead tries to find a DNS name or IP address for this node (according to the strategy established by your NNMi administrator).</p> <p>For example, when an SNMP agent responds with a default sysName, NNMi's maps might display multiple icons with the same name (one for every device of that type in your environment that responded to an SNMP query with the default sysName). Usually, the device administrator changes the default sysName value to something more meaningful, so this problem is avoided.</p>
<b>Device Behaviors</b>	
Force Device	<p>This attribute enables the NNMi administrator to override the IP Forwarding (Layer 3) and LAN Switching (Layer 2) settings provided by Spiral Discovery (displayed on the <a href="#">"Node Form: Capabilities Tab" (on page 35)</a>).</p> <p>Possible values are:</p> <ul style="list-style-type: none"> <li>• Force to router</li> <li>• Force to switch</li> <li>• Force to end node</li> <li>• Force to switch and router</li> </ul> <p>An NNMi administrator might want to use this attribute to override the IP Forwarding (Layer 3) and LAN Switching (Layer 2) capabilities setting for the device under the following circumstances:</p> <ul style="list-style-type: none"> <li>• The sysServices setting in the MIB that is used to determine the IP Forwarding (Layer 3) and LAN Switching (Layer 2) capability during discovery is not accurate due to an IOS defect on the device</li> <li>• The device serves as a router, switch, or switch and router and the NNMi administrator wants to force the device to be treated as only one of the following: 1) a router, 2) a switch, or 3) a switch and router.</li> </ul> <p>Devices whose <b>Force Device</b> attribute is set to either of the following are included in Layer 3 Neighbor View maps: 1) Force to router or 2) Force to switch and router.</p> <ul style="list-style-type: none"> <li>• The device serves as a virtual router, but should not be managed as a router.</li> </ul> <p>Setting the Force Device attribute to <b>Force to end node</b> enables the NNMi administrator to configure discovery so NNMi ignores this device.</p>
Interface Reindexing Type	<p>When an interface within a device changes (old one removed, new one added), the interface index number changes. State Poller uses the attribute specified here to detect the</p>

Attribute	Description
	change. Your NNMi administrator chooses which interface attribute indicates a change: ifIndex, ifName, ifDescr, ifAlias, or a combination of ifName and ifDescr. See the General Interface Attributes (SNMP Values) in <a href="#">Interface Form</a> for more information.

## Device Family Form

The Device Family attribute value indicates the family name assigned by the vendor when the device was manufactured; for example, the Cisco Catalyst 6500 Series Switches.

- NNMi monitoring behavior can be configured differently for each family.
- Membership in a Node Group can be determined by device family.

This form is accessed from the "[Device Profile Form](#)" (on page 56).

### Device Family Definition

Attribute	Description
Label	Device family name. For example, Cisco Catalyst 6500 Series Switches or HP Advance-Stack Routers.  Maximum length 255 characters. Alpha-numeric, punctuation, spaces, and underline characters allowed.
Unique Key	The required unique identifier that is important when exporting and importing device profile information within NNMi.  The value must be unique. One possible strategy is to use the Java name space convention. For example:  <code>com.&lt;your_company_name&gt;.nnm.deviceProfile.family.&lt;family_label&gt;</code>  Maximum length 80 alpha-numeric characters. Periods allowed. No spaces allowed.
Management URL	<i>Optional.</i> The URL to the device's management page (provided by the vendor). This page is used to provide configuration information for the device and is usually organized by device family.

## Device Vendor Form

The Device Vendor attribute value indicates the name of the manufacturer of this device type; for example, HP or Cisco.

- NNMi monitoring behavior can be configured differently for each vendor.
- Membership in a Node Group can be determined by device vendor.

This form is accessed from the "[Device Profile Form](#)" (on page 56).

### Device Vendor Definition

Attribute	Description
Label	Vendor name.  Maximum length 255 characters. Alpha-numeric, punctuation, spaces, and underline characters allowed.

Attribute	Description
Unique Key	<p>The required unique identifier that is important when exporting and importing device profile information within NNMi.</p> <p>The value must be unique. One possible strategy is to use the Java name space convention. For example:</p> <pre>com.&lt;your_company_name&gt;.nnm.deviceProfile.vendor.&lt;vendor_label&gt;</pre> <p>Maximum length 80 alpha-numeric characters. Periods allowed. No spaces allowed.</p>

## Device Category Form

The Device Category attribute value indicates the category of this device; for example, router, switch, or printer. This attribute:

- In Map views, determines which background shape NNMi uses for the icon representing devices of this type.
- In table views, the category value can be used when sorting/filtering the Category column.
- During discovery, NNMi behavior changes based on the device category. For example, routers and switches are discovered by default.
- NNMi monitoring behavior can be configured differently for each category.
- Membership in a Node Group can be determined by device category.

This form is accessed from the ["Device Profile Form" \(on page 56\)](#).

## Device Category Definition

Attribute	Description
Label	<p>Category name.</p> <p>Maximum length 255 characters. Alpha-numeric, punctuation, spaces, and underline characters allowed.</p>
Unique Key	<p>The required unique identifier that is important when exporting and importing device profile information within NNMi.</p> <p>The value must be unique. One possible strategy is to use the Java name space convention. For example:</p> <pre>com.&lt;your_company_name&gt;.nnm.deviceProfile.category.&lt;category_label&gt;</pre> <p>Maximum length 80 alpha-numeric characters. Periods allowed. No spaces allowed.</p>

## Device Profile Author Form

The Author attribute value indicates who created the device profile.

This form is accessed from the ["Device Profile Form" \(on page 56\)](#).

## Device Category Author

Attribute	Description
Label	Author name. If your NNMi administrator modified the default Device Profile provided by

Attribute	Description
	<p>NNMi, a value other than HP Network Node Manager should appear.</p> <p>Maximum length 255 characters. Alpha-numeric, punctuation, spaces, and underline characters allowed.</p>
Unique Key	<p>The required unique identifier that is important when exporting and importing device profile information within NNMi.</p> <p>The value must be unique. One possible strategy is to use the Java name space convention. For example:</p> <pre>com.&lt;your_company_name&gt;.nnm.deviceProfile.author.&lt;author_label&gt;</pre> <p>Maximum length 80 alpha-numeric characters. Periods allowed. No spaces allowed.</p>

## Interface Form

The Interface form provides details about the network interface selected. From this form you can access more details about the parent [node](#), [addresses](#), current [network connection](#), and [incidents](#) associated with this interface.







If your role allows, you can use this form to modify the [Management Mode](#) for an interface (for example to indicate it will be temporarily out of service) or add [notes](#) to communicate information about this interface to your team.











If you see several blank fields for an interface in a form, the interface is a Nortel private interface. This means the following:


- The interface has no information in the MIB file.
- NNMi is not able to access the information that is normally available for other interfaces. Only limited attributes can be determined. Possible attribute values that might be collected include the MAC address and interface index.

For information about each tab:

### Basic Attributes

Attribute	Description
Name	The most accurate interface name available to the initial discovery process. First choice is the IF MIB <code>ifName</code> value. Second choice is the <code>ifAlias</code> value. Third choice is a combination of the <code>ifType[ifIndex]</code> value (for example, <code>ethernetCsmacd[17]</code> ).
Status	<p>Overall status for the current interface. NNMi follows the ISO standard for status classification. See the <a href="#">"Interface Form: Status Tab" (on page 72)</a> for more information. Possible values are:</p> <ul style="list-style-type: none"> <li> No Status</li> <li> Normal</li> <li> Disabled</li> <li> Unknown</li> <li> Warning</li> <li> Minor</li> </ul>









Attribute	Description
	<p> Major</p> <p> Critical</p> <p>Interface status is derived from SNMP polling results for <a href="#">ifAdminStatus</a> and <a href="#">IfOperStatus</a>, as well as from any conclusions. Status reflects the most serious outstanding conclusion. See the <a href="#">"Interface Form: Conclusions Tab" (on page 73)</a> for information about how the current status was determined. See <a href="#">"Watch Status Colors" (on page 129)</a> for more information about possible status values.</p> <p><b>Note:</b> The icons are displayed only in table views.</p>
Management Mode	<p>The calculated Management Mode for the interface. This value should reflect the management mode assigned to the node on which the selected interface resides. For example, if the node's management mode is <b>Managed</b>, and the Direct Management Mode of the interface is <b>Inherited</b>, the interface Management Mode value is <b>Managed</b>.</p>
Direct Management Mode	<p>Indicates whether the current interface is being managed. This attribute is set by the administrator and specifies whether an interface should be managed or whether an interface is temporarily out of service. Possible values are:</p> <p> <b>Inherited</b> – Used to indicate that the interface should inherit the Management Mode from the node on which it resides.</p> <p> <b>Not Managed</b> – Used to indicate that NNMi does not discover or monitor the interface. For example, the interface might not be accessible because it is in a private network.</p> <p> <b>Out of Service</b> – Used to indicate an interface is unavailable because it is out of service. NNMi does not discover or monitor these interfaces.</p> <p>This attribute is useful for notifying NNMi when an interface is temporarily out of service, or should never be managed.</p> <p><b>Note:</b> If you change the Direct Management Mode, NNMi updates the calculated Management Mode on the form. If you manually set the Direct Management Mode and then Save your changes, the Management Mode value is not updated until you refresh the form.</p>
Hosted On Node	<p>Node on which the interface resides. This is the current value in the NNMi database for the Name attribute of the host device. The value could be a DNS name, a MIB II sysName, or an address (depending on how your NNMi administrator configured the discovery process).</p> <p>Click the  Lookup icon and select  Quick View or  Open to display more information about the node.</p>
Physical Address	<p>The interface address at the physical layer, also known as the MAC address. This is the globally unique serial number assigned to each interface at the factory.</p>
Layer 2 Connection	<p>Used to indicate whether the selected interface is part of a Layer 2 connection. If the interface is part of a connection, use this attribute to access information about its Layer 2 connection and the neighboring device. Click here for instructions.</p> <ol style="list-style-type: none"> <li>1. Navigate to the <b>Layer 2 Connection</b> attribute. Click the  Lookup icon, and select  Open.</li> </ol>

Attribute	Description
	<ol style="list-style-type: none"> <li>2. In the Layer 2 Connection form, locate the <b>Interfaces</b> tab.</li> <li>3. Click the  Open icon of the other interface participating in this connection.</li> <li>4. In the <b>Interface</b> form, locate the <b>Hosted On Node</b> attribute.</li> <li>5. The Node form contains all known information about the neighboring node.</li> </ol>

### Interface State Attributes







**Administrative State** Either the current MIB II ifAdminStatus value (set by the device's administrator) or a value calculated by the State Poller Service. The current Administrative State contributes towards the status calculation for this interface. See the ["Interface Form: Status Tab" \(on page 72\)](#) for more information.







Possible values are:

-  **Up** – The SNMP agent responded with an ifAdminStatus value of Up.
-  **Down** – The SNMP agent responded with an ifAdminStatus value of Down.
-  **Testing** – The SNMP agent responded with an ifAdminStatus value of Testing.
-  **Other** – The SNMP agent responded with a value for ifAdminStatus that is not recognized.
-  **Unavailable** – The SNMP agent responded, but returned a null value for the ifAdminStatus request.
-  **Not Polled** – Indicates that this interface is intentionally not polled, based on current Monitoring Configuration settings, current Communication Configuration settings, or because the Interface or parent Node is set to Not Managed or Out of Service.
-  **Agent Error** – Indicates an SNMP error was returned in response to an SNMP query to this agent.
-  **No Polling Policy** – Indicates that this interface is not included in any internal NNMi polling policies, and therefore not polled for this information.

**Operational State** Either the current MIB II ifOperStatus value or a value calculated by the State Poller Service. The current Operational State contributes towards the status calculation for this interface. See the ["Interface Form: Status Tab" \(on page 72\)](#) for more information.

Possible values are:

-  **Up** – The SNMP agent responded that the interface is operationally up, ready to receive and send network traffic.
-  **Down** – The SNMP agent responded that the interface is operationally down.
-  **Testing** – The SNMP agent responded that the interface is in test mode.
-  **Other** – The SNMP agent responded with a value for ifOperStatus that is not recognized.
-  **Unknown** – The SNMP agent responded with an ifOperStatus value of Unknown.
-  **Dormant** – Indicates the SNMP agent responded that the interface is in a "pending"

Attribute	Description
	<p>state, waiting for some external event.</p> <p> <b>Not Present</b> – Indicates that the interface is missing some hardware component.</p> <p> <b>Lower Layer Down</b> – Indicates the interface is down due to the state of lower-level interfaces.</p> <p> <b>Unavailable</b> – The SNMP agent responded, but returned a null value for the ifOperStatus request.</p> <p> <b>Not Polled</b> – Indicates that this interface is intentionally not polled, based on current Monitoring Configuration settings, current Communication Configuration settings, or because the Interface or parent Node is set to Not Managed or Out of Service.</p> <p> <b>Agent Error</b> – Indicates an SNMP error was returned in response to an SNMP query to this agent.</p> <p> <b>No Polling Policy</b> – Indicates that this interface is not included in any internal NNMi polling policies, and therefore not polled for this information.</p>
State Last Modified	Indicates the date and time when the Administrative State, Operational State, or both were last modified.
Notes	<p>Provided for network operators to use for any additional notes required to further explain the interface. Information might include to what service or customer the interface is connected.</p> <p>Type a maximum of 1024 characters. Alpha-numeric, punctuation, spaces, and underline characters are allowed.</p> <p><b>Note:</b> You can sort your interface table views based on this value. Therefore, you might want to include keywords for this attribute value.</p>

## Interface Form: General Tab

The "[Interface Form](#)" (on page 60) provides details about the selected network interface.

For information about each tab:

### General SNMP Values

Attribute	Description
IfName	Optional Interface MIB variable for ifName assigned to the interface by the vendor. If no IfName value is provided, SNMP uses the ifType+ifIndex which is dynamically configured and can change. This name is not guaranteed to be unique or consistent across reboots.
IfAlias	Optional Interface MIB variable for ifAlias assigned to the interface. This value is set by the device administrator. An ifAlias could be useful if the interface vendor did not provide an ifName value.
IfDescription	Optional Interface MIB variable for ifDescr for the interface. This attribute is set by the device administrator.
IfIndex	Interface MIB variable for the row number in the interface table (ifTable) for this interface. The row number can change with each reboot.  <b>Note:</b> Interfaces on non-SNMP nodes have an ifIndex value of 0 (zero).


Attribute	Description
IfSpeed	Interface MIB variable for the interface's bandwidth in bits per second. Depending on the device vendor, this value may indicate current speed or potential speed.
IfType	Interface MIB variable for the physical link protocol type of the interface. Possible values include: Ethernet and frameRelay.  <b>Note:</b> Interfaces on non-SNMP nodes have an ifType value of <b>other</b> .
Input Speed	Indicates the speed at which an interface is capable of receiving data in bits per second ("Gbps", "Mbps").  You can type a value to override the ifSpeed value returned by the device's SNMP agent. NNMi retains the value you enter.  A reason you might want to override this value include the following:  Sometimes the value returned by the device's SNMP agent is not accurate or causes problems when NNMi calculates performance monitoring. For example, the input speed might be restricted due to circumstances in your environment, or bandwidth controls might limit the connection speed regardless of what the physical connection is capable of (such as within a WAN).
Output Speed	Indicates the speed at which an interface is capable of transmitting data in bits per second ("Gbps", "Mbps").  You can type a value to override the output speed value returned by the device's SNMP agent. NNMi retains the value you enter.  A reason you might want to override this value include the following:  Sometimes the value returned by the device's SNMP agent is not accurate or causes problems when NNMi calculates performance monitoring. For example, the output speed might be restricted due to circumstances in your environment, or bandwidth controls might limit the connection speed regardless of what the physical connection is capable of (such as within a WAN).

## Interface Form: IP Addresses Tab

The ["Interface Form" \(on page 60\)](#) provides details about the selected network interface.

**For information about each tab:**

### IP Addresses Table

Attribute	Description
IP Address	Table view of the IP addresses associated with the selected interface. You can use this table to determine the state and address for each IP address.  Click the  Open icon to open the <a href="#">"IP Address Form" (on page 73)</a> and view more information about a specific address.


## Interface Form: VLAN Ports Tab

The ["Interface Form" \(on page 60\)](#) provides details about the selected network interface.

**For information about each tab:**



## VLAN Ports Table

Attribute	Description
VLAN Ports	<p>Table view of all of the VLAN ports associated with the current interface. Use this table to determine all port and VLAN combinations associated with this interface.</p> <p>Click the  Open icon to open the Port Form and view more information about a specific VLAN port.</p>

## Interface Form: Link Aggregation Tab (NNMi Advanced)

The "Interface Form" (on page 60) provides details about the selected network interface.

For more information about each tab:



The Interface Form: Link Aggregation Tab appears if the selected interface participates in a **Link Aggregation**<sup>1</sup> protocol. The contents of the tab differ based on the Interface role in the Link Aggregation (Member or Aggregator).

A Member Interface's Link Aggregation Tab displays the Link Aggregation protocol and a reference to the Aggregation's Aggregator Interface. Click here for more details about the attributes displayed.

### Link Aggregation Tab


Attribute	Description
Link Aggregation Protocol	<p>Protocol used to create the Link Aggregation, including the Aggregator Interface and its physical Members. Possible values include:</p> <ul style="list-style-type: none"> <li>• Cisco Systems Port Aggregation Protocol (pagp)</li> <li>• Multi-Link Trunk technology (mlt)</li> <li>• Split Multi-Link Trunk technology (smlt)</li> <li>• Inter-switch trunk that is part of a Split Multi-Link Trunk configuration (istMlt)</li> </ul>
Aggregator	<p>Name of the Aggregator Interface for the selected physical Member Interface. The Aggregator Interface represents the collection of physical interfaces for one end of a Link Aggregation.</p> <p>See <a href="#">Layer 2 Neighbor View Map Objects</a> for more information.</p> <p>This name will be the most accurate interface name available to the initial discovery process. First choice is the IF MIB <code>ifName</code> value. Second choice is the <code>ifAlias</code> value. Third choice is a combination of the <code>ifType[ifIndex]</code> value (for example, <code>eth-ernetCsmacd[17]</code>).</p>

<sup>1</sup>A Link Aggregation is comprised of an Aggregator Link, Aggregator Interface, and the physical interfaces and connections that they represent. An Aggregator Link object represents many-to-many physical connections. For example, two nodes might be connected with four physical connections. These four physical connections are depicted as a single Aggregator Link object using a thick line on the Layer 2 Neighbor View map. The interface depicted at each end of the Aggregator Link object is an Aggregator Interface object. An Aggregator Interface object represents the collection of physical interfaces for one end of an Aggregator Link.

Attribute	Description
	Click the  Lookup icon, and choose  Open to open the form for the Aggregator Interface.

The Aggregator Interface's Link Aggregation Tab lists the Member Interfaces of its end of the Link Aggregation and provides cumulative bandwidth statistics. Click here more details about the attributes displayed.

### Link Aggregation Tab

Attribute	Description
Link Aggregation Protocol	<p>Protocol used to create the Link Aggregation, including the Aggregator Interface and its physical Members.</p> <p>Possible values include:</p> <ul style="list-style-type: none"> <li>• Cisco Systems Port Aggregation Protocol (pagp)</li> <li>• Multi-Link Trunk technology (mlt)</li> <li>• Split Mutli-Link Trunk technology (smlt)</li> <li>• Inter-switch trunk that is part of a Split Multi-Link Trunk configuration (istMlt)</li> </ul>
Available Bandwidth	Sum of the interface Input Speed attribute values of the Member Interfaces whose MIB II ifOperStatus is not <code>Down</code> . If the sum of the interface Output Speed attribute values is different, NNMi displays separate Available Input Bandwidth and Available Output Bandwidth attributes.
Maximum Bandwidth	Sum of the interface Input Speed attribute values of the Member Interfaces, regardless of MIB II ifOperStatus . If the sum of the interface Output Speed attribute values is different, NNMi displays separate Maximum Input Bandwidth and Maximum Output Bandwidth attributes.
Available Bandwidth Percentage	Percentage value computed using Available Bandwidth divided by the Maximum Bandwidth.
Members	<p>Table view of the physical Member Interfaces.</p> <p>Click the  Open icon to view more information about a specific interface.</p>

### Interface Form: Capabilities Tab

The Interface Form: Capabilities Tab displays a table view of any capabilities added to the interface object by NNMi or an external application. For example, NNMi uses the capability feature to identify interfaces for which NNMi can obtain only limited information. Examples of these interfaces include Nortel interfaces as well as any interface on a non-SNMP node. To help identify these interfaces, NNMi assigns the interface the capability of `com.hp.nnm.capability.iface.private`.

**Note:** Because the values are generated by NNMi or an external application, Capability values cannot be modified.

**For information about each tab:**

## Capabilities Table

Attribute	Description
Capability	<p>The name of the capability added to an interface object by either NNMi or an external application. For more information, see:</p> <ul style="list-style-type: none"> <li>• <a href="#">"Interface Capability Form" (on page 69)</a></li> <li>• <a href="#">"Interface Capabilities Provided by NNMi" (on page 67)</a></li> </ul>
Unique Key	<p>The database identifier for the capability that either NNMi or an external application added to this interface.</p> <p><b>Note:</b> Capabilities added by NNMi use a Unique Key value that begins with the prefix: <code>com.hp.nnm.capability</code>. See <a href="#">"Interface Capabilities Provided by NNMi" (on page 67)</a> for a description of the capabilities provided by NNMi that might appear under the Interface Form: Capabilities Tab.</p>

## Interface Capabilities Provided by NNMi

The Interface Form: Capabilities Tab displays a table view of any capabilities that have been added to the interface object. Capabilities that begin with `com.hp.nnm.capability` represent capabilities that NNMi provides. External applications can also add interface capabilities.

### NNMi Interface Capabilities

Capability	Unique Key	Description
Private	<code>com.hp.nnm.capability.iface.private</code>	<p>Indicates the interface was discovered in either a non-SNMP node or a Nortel node. Private interfaces are not monitored for Status.</p> <p>For interfaces on non-SNMP nodes, note the following:</p> <ul style="list-style-type: none"> <li>• The interface index (<code>ifIndex</code>) value is always set to <b>0</b> (zero).</li> <li>• The interface type (<code>ifType</code>) is set to <b>Other</b>.</li> <li>• The interface Name (<code>ifName</code>), if none is available, is set to <b>Pseudo Interface</b>.</li> <li>• If the interface hosts an IP address, the interface Alias (<code>ifAlias</code>) is set to the IP address. Otherwise, the interface Alias (<code>ifAlias</code>) is set with information from neighboring SNMP devices.</li> <li>• NNMi obtains the MAC address if the IP address can be resolved using ARP cache.</li> </ul> <p>Note the following about <b>Pseudo</b> interfaces: NNMi attempts to obtain additional information using a variety of discovery protocols.</p> <p>For Nortel SNMP interfaces, note the following:</p>

Capability	Unique Key	Description
		<ul style="list-style-type: none"> <li>The ifindex value is set according the Nortel private MIB.</li> <li>NNMi tries to collect the MAC address and interface name using Nortel's private MIBs.</li> </ul>

**NNMi Advanced.** The capabilities in the following table identify whether the interface participating in a Link Aggregation is an aggregator or member.

**NNMi Advanced. Link Aggregation Interface Capabilities: Roles**

Capability	Unique Key	Description
Aggregate Interface	<code>com.hp.nnm.capability.lag.aggregator</code>	Indicates the interface represents the collection of physical interfaces for one end of an Aggregator Link.  See <a href="#">Layer 2 Neighbor View Map Objects</a> for more information.
Aggregate Member	<code>com.hp.nnm.capability.lag.member</code>	Indicates the interface is a physical interface that is a member of an Aggregator Interface.  See <a href="#">Layer 2 Neighbor View Map Objects</a> for more information.

**NNMi Advanced.** The capabilities in the following table are used to identify the Link Aggregation protocol used.

**NNMi Advanced. Link Aggregation Interface Capabilities: Protocols**

Capability	Unique Key	Description
Cisco Port Aggregation Protocol	<code>com.hp.nnm.capability.lag.protocol.pagp</code>	Indicates an interface using Cisco Systems Port Aggregation Protocol.
Inter-Switch Trunk MLT	<code>com.hp.nnm.capability.lag.protocol.istmlt</code>	Indicates an inter-switch trunk that is part of a Split Multi-Link Trunk configuration.
Nortel Multi-Link Trunking	<code>com.hp.nnm.capability.lag.protocol.mlt</code>	Indicates an interface using the Multi-Link Trunk technology.
Split MLT	<code>com.hp.nnm.capability.lag.protocol.smlt</code>	Indicates an interface using Split Multi-Link Trunk technology.
Static/Manual Configured Link Aggregation	<code>com.hp.nnm.capability.lag.protocol.static</code>	Indicates the Cisco device has been manually configured for aggregation.

## Interface Capability Form

This form describes a capability added to the interface object by NNMi or an external application. For example, NNMi uses the capability feature to identify interfaces for which NNMi can obtain only limited information. Examples of these interfaces include Nortel interfaces as well as any interface on a non-SNMP node. To help identify these interfaces, NNMi assigns the interface the capability of `com.hp.nnm-capability.iface.private`.

**Note:** Because the values are generated by NNMi or an external application, Capability values cannot be modified.

Each Capability attribute is described in the table below.

### Basics Attributes

Attribute	Description
Capability	Label used to identify the Capability that was added to the interface object. The Capability value is listed in the table on the Capabilities tab in an Interface form. See <a href="#">"Interface Form: Capabilities Tab" (on page 66)</a> .
Unique Key	Used as a unique identifier for the Capability. Any capability provided by NNMi begins with the prefix <code>com.hp.nnm.capability</code> .  <b>Note:</b> Capabilities added by NNMi use a Unique Key value that begins with the prefix: <code>com.hp.nnm.capability</code> . See <a href="#">"Interface Capabilities Provided by NNMi" (on page 67)</a> for a description of the capabilities provided by NNMi that might appear under the Interface Form: Capabilities Tab.

## Interface Form: Custom Attributes Tab

Custom Attributes enable an NNMi administrator to add information to the Interface object. Custom Attributes can also be set by external applications that have been integrated with NNMi.

The Interface Form: Custom Attributes Tab displays a table view of any Custom Attributes that have been added to the interface object. For example, your NNMi administrator might have added **Role** as another attribute for the interfaces in your network.

**Note:** If your role allows, you can edit a Custom Attribute. Only users assigned to the NNMi Administrator role can add a Custom Attribute.

### Custom Attributes Table

Attribute	Description
Name	Name used to identify the Custom Attribute. This name appears in the table view on the Custom Attributes tab in Interface forms.
Value	The actual value for the Custom Attribute for the selected interface. For example, the value for <b>Role</b> might be <b>WAN interface to the London office</b> . For more information, see <a href="#">"Interface Capabilities Provided by NNMi" (on page 67)</a> .

## Interface Custom Attributes Form

Custom Attributes enable an NNMi administrator to add information to the interface object. For example, your NNMi administrator might have added **Role** as another attribute for the interfaces in your network.

Custom Attributes can also be set by external applications that have been integrated with NNMi.

The Custom Attributes form displays the Name and Value for each of the Custom Attributes that were added to the interface object. Each of these attributes is described in the table below.

### Basics Attributes


Attribute	Description
Name	Name used to identify the Custom Attribute. This name appears in the table view on the Custom Attributes tab in the Interface forms.
Value	Value assigned to the Custom Attribute for the selected interface object. For example, the value for <b>Role</b> might be <b>WAN interface to the London office</b> .

### Interface Form: Interface Groups Tab

The "[Interface Form](#)" (on page 60) provides details about the selected network interface.

For information about each tab:

#### Interface Groups Membership Table

Attribute	Description
Interface Groups	Table view of Interface Groups to which the selected interface belongs. Interface groups are based on specific characteristics of interfaces.  Click the  Open icon to view more information about a specific Interface Group.







### Interface Form: Performance Tab (NNM iSPI Performance for Metrics)


The "[Interface Form](#)" (on page 60) provides details about the selected network interface.

For information about each tab:

The Performance tab displays data if the NNM iSPI Performance for Metrics software is installed and configured within your environment. The NNMi administrator can configure an optional high/low threshold.

The icons on the Performance tab indicate the value of the most recent interface performance states:

 <b>High</b> - The High threshold was crossed.	 <b>Not Polled</b> - Indicates that this interface is intentionally not polled. Possible reasons are: Performance Monitoring is not enabled, because of current Communication Configuration settings in NNMi, or because the parent Node or Interface is set to Not Managed or Out of Service.
 <b>Nominal</b> - Measured within healthy range. (Or no thresholds are being monitored.)	 <b>Unavailable</b> - Unable to compute the performance state or the computed value is outside of the valid range (0.00 - 100.00).
 <b>Low</b> - The Low threshold was crossed.	 <b>Agent Error</b> - The SNMP agent responded with an error, rather than a value.

 **None** - The value returned was zero.

### Performance Results Table (NNM iSPI Performance for Metrics)


Attribute	Description
Input Utilization	<p>The total number of incoming octets traversing the interface as a percentage of the total possible number of octets (based on the ifSpeed value). From Interface to Interface, the exact MIB variables queried vary based on interface speed and whether the system supports the high speed counters for interfaces.</p> <p><b>Tip:</b> Sometimes the value returned by the device's SNMP agent is not accurate and causes problems when NNMi calculates input utilization. NNMi lets you manually override the ifSpeed provided by the SNMP agent for this interface. See <a href="#">Input Speed</a>.</p>
Output Utilization	<p>For full-duplex interfaces, the total number of outbound octets traversing the interface as a percentage of the total possible number of octets (based on the ifSpeed value). From Interface to Interface, the exact MIB variables queried vary based on interface speed and whether the system supports the high speed counters for interfaces.</p> <p><b>Tip:</b> Sometimes the value returned by the device's SNMP agent is not accurate and causes problems when NNMi calculates output utilization. NNMi lets you manually override the output speed provided by the SNMP agent for this interface. See <a href="#">Output Speed</a>.</p>
Input Error Rate	<p>Percentage based on the reported change in the number of input packets on the interface and the packet error count. What constitutes an error is system specific, but likely includes such issues as bad packet checksums, incorrect header information, and runt packets.</p>
Output Error Rate	<p>Percentage based on the reported change in the number of output packets on the interface and the packet error count. What constitutes an error is system specific, but likely includes such issues as collisions and buffer errors.</p>
Input Discard Rate	<p>Percentage based on the reported change in the number of input packets on the interface and the discarded packet count. Packets may be discarded because of a variety of issues, including receive buffer overflows, congestion, or system specific issues.</p>
Output Discard Rate	<p>Percentage based on the reported change in the number of output packets on the interface and the discarded packet count. Packets may be discarded because of a variety of issues, including transmission buffer overflows, congestion, or system specific issues.</p>

### Interface Form: Incidents Tab

The "[Interface Form](#)" (on page 60) provides details about the selected network interface.

For information about each tab:

#### Incidents Table

Attribute	Description
Associated Incidents	<p>Table view of the incidents associated with the selected interface. These incidents are sorted by creation time so that you can view the incidents in chronological order. Use this view to determine which incidents are still open for the selected interface.</p> <p>Click the  Open icon to open the "<a href="#">Incident Form</a>" (on page 134) and view more infor-</p>










Attribute	Description
	mation about a specific incident.

## Interface Form: Status Tab

The "[Interface Form](#)" (on page 60) provides details about the selected network interface.

For information about each tab:

### Status Tab

Attribute	Description
Status	<p>Overall status for the current interface. NNMi follows the ISO standard for status classification. Possible values are:</p> <ul style="list-style-type: none"> <li> No Status</li> <li> Normal</li> <li> Disabled</li> <li> Unknown</li> <li> Warning</li> <li> Minor</li> <li> Major</li> <li> Critical</li> </ul> <p>Interface status is derived from SNMP polling results for <a href="#">ifAdminStatus</a> and <a href="#">IfOperStatus</a>, as well as any conclusions. For information about how the current status was determined, see the "<a href="#">Interface Form: Conclusions Tab</a>" (on page 73). Status reflects the most serious outstanding conclusion. See "<a href="#">Watch Status Colors</a>" (on page 129) for more information about possible status values.</p> <p><i>NNMi Advanced.</i> If the interface is an Aggregator Interface, the Status is calculated using the Status of the Aggregator Interface members. Click here for more information.</p> <p>A Status of <b>Minor</b> indicates the Status of at least one of the Aggregator Interface members is <b>Critical</b>. A Status of <b>Critical</b> indicates the Status of all the Aggregator Interface members is <b>Critical</b>.</p> <p>Also see <a href="#">Layer 2 Neighbor View Map Objects</a>.</p> <p><b>Note:</b> The icons are displayed only in table views.</p>
Status Last Modified	Date and time indicating when the status was last set.
Status History	<p>List of up to the last 30 changes in the status for the interface. This view is useful for obtaining a summary of the interface status so that you can better determine any patterns in behavior and activity.</p> <p>Click the  Open icon to view more information about a specific status.</p>




## Interface Form: Conclusions Tab

The "[Interface Form](#)" (on page 60) provides details about the selected network interface.

For information about each tab:

### Conclusions Table for Status Calculations

Attribute	Description
Outstanding Status Conclusions	<p>The dynamically generated list of summary statuses of the interface at points in time that contributed to the current overall status of the selected interface. Status is set by the Causal Engine.</p> <p>Each conclusion listed is still outstanding and applies to the current overall status.</p> <p>This view is useful for obtaining a quick summary of the status and problem description for the current node's interfaces that led up to the node's most current status.</p> <p>Examples of conclusions that might appear together are listed below:</p> <ul style="list-style-type: none"><li>• SNMP Agent Not Responding</li><li>• Interface Down</li><li>• Address Down</li></ul> <p>The status value is correlated based on the most critical conclusions.</p> <p>Click the  Open icon to view more information about a specific conclusion.</p>

## Interface Form: Registration Tab

The "[Interface Form](#)" (on page 60) provides details about the selected network interface.

For information about each tab:

### Registration

Attribute	Description
Created	Date and time the selected object instance was created. NNM uses the locale of the client and the date and time from the NNMi management server.
Last Modified	Date the selected object instance was last modified. NNM uses the locale of the client and the date and time from the NNMi management server.








## IP Address Form








The IP Address form provides information for the IP address selected. This form is useful for troubleshooting purposes because you can access additional information about the [node](#), [interface](#), [subnet](#), and [incidents](#) associated with this address.

If your role allows, you can use this form to modify the [Management Mode](#) for an address (for example, to indicate it will be temporarily out of service) or add [notes](#) to communicate information about this address to your team.

For information about each tab:

## Basic Attributes

Attribute	Description
Address	An IP address provided by your NNMi administrator as a discovery seed or an IP address gathered by Spiral Discovery.
Prefix Length	The number of significant bits in the subnet prefix associated with this IP address. For IPv4 addresses, this value is derived from the subnet mask.
Status	Overall status for the current IP address. NNMi follows the ISO standard for status classification. See <a href="#">"IP Address Form: Status Tab" (on page 75)</a> .
Management Mode	The calculated Management Mode for the address used to indicate whether the current IP address is being managed.  This value should reflect the management mode assigned to the node on which the selected address resides as well as on any associated interfaces. For example, if the node's management mode is <b>Managed</b> , and the Management Mode of the interface is <b>Inherited</b> , the Management Mode value for the address is <b>Managed</b> .
Direct Management Mode	This attribute is set by the administrator and specifies whether an address should be managed or is temporarily out of service. Possible values are:   <b>Inherited</b> – Used to indicate that the address should inherit the Management Mode from the associated interface, if any. Otherwise the address inherits the Management Mode of the node on which it resides.   <b>Not Managed</b> – Used to indicate that you do not plan to manage the address. For example, the address might not be accessible because it is in a private network. NNMi does not discover or monitor these addresses.   <b>Out of Service</b> – Used to indicate the address is unavailable because it is out of service. NNMi does not discover or monitor these addresses.  This attribute is useful for notifying NNMi when an address is been temporarily out of service, or should never be managed.  <b>Note:</b> If you change the Direct Management Mode, NNMi updates the calculated Management Mode on the form. If you manually set the Direct Management Mode and then Save your changes, the Management Mode value is not updated until you refresh the form.
State	Indicates whether the IP address is available and how NNMi is using SNMP to interact with this IP address. Possible values are:   <b>Responding</b> – Indicates that the IP address is being polled and is responding to an ICMP ping.   <b>Not Responding</b> – Indicates that the IP address is being polled, but is not responding to an ICMP ping.   <b>Not Polled</b> – Indicates that this IP address is intentionally not polled, based on current Monitoring Configuration settings, current Communication Configuration settings, or because the IP Address, parent Interface, or parent Node is set to Not Managed or Out of Service.   <b>No Polling Policy</b> – Indicates that this address is not included in any Monitoring Configuration settings, and therefore not polled.

Attribute	Description
	<p><b>Note:</b> NNMi's State Poller determines the State. The current state contributes towards the status calculation for the address. See the <a href="#">Status tab</a> for more information.</p>
State Last Modified	Indicates the date and time when the State value was last modified.
In Interface	MIB II ipAddrTable value indicating the interface that owns this IP address. Click the  ▾ Lookup icon and select  Open to display more information about the interface.
Hosted On Node	<p>Node on which the address resides. This is the current value in NNMi's database for the Name attribute of the host device. The value could be a DNS name, a MIB II sysName, or an address (depending on how your NNMi administrator configured the discovery process).</p> <p>Click the  ▾ Lookup icon and select  Quick View or  Open to display more information about the node.</p>
In Subnet	Subnet on which the IP address resides. NNMi derives this subnet based on the IP address and the subnet prefix information. Click the  ▾ Lookup icon and select  Open to display more information about the IP subnet.
Notes	<p>Provided for network operators to use for any additional notes required to further explain the IP address. Information might include whether the address is a backup address. You might also use this attribute to track which geographical group might use the address.</p> <p>Type a maximum of 1024 characters. Alpha-numeric, punctuation, spaces, and underline characters are allowed.</p> <p><b>Note:</b> You can sort your IP address table views based on this value. Therefore, you might want to include keywords for this attribute value.</p>


## IP Address Form: Incidents Tab

**Tip:** See "[Incident Form](#)" (on page 134) for more details about the incident attributes that appear in the incident view's column headings.

The "[IP Address Form](#)" (on page 73) provides details about the selected IP address.

**For information about each tab:**

### Incidents Table










Description
<p>Table view of the incidents associated with the selected address. These incidents are sorted by creation time so that you can view the incidents in chronological order. Use this view to determine which incidents are still open for the selected address.</p> <p>Click the  Open icon to open the "<a href="#">Incident Form</a>" (on page 134) and view more information about a specific incident.</p>

## IP Address Form: Status Tab

The "[IP Address Form](#)" (on page 73) provides details about the selected IP address .

For information about each tab:

### Status of this IP Address

Attribute	Description
Status	<p>Overall status for the current IP address. NNMi follows the ISO standard for status classification. Possible values are:</p> <ul style="list-style-type: none"> <li> No Status</li> <li> Normal</li> <li> Disabled</li> <li> Unknown</li> <li> Warning</li> <li> Minor</li> <li> Major</li> <li> Critical</li> </ul> <p>IP address status is derived from ICMP ping results, as well as any conclusions. For information about how the current status was determined, see the <a href="#">"IP Address Form: Conclusions Tab" (on page 76)</a>. Status reflects the most serious outstanding conclusion. See <a href="#">"Watch Status Colors" (on page 129)</a> for more information about possible status values.</p> <p><b>Note:</b> The icons are displayed only in table views.</p>
Status Last Modified	Indicates the date and time when the Status value was last modified.
Status History	<p>List of up to the last 30 changes in status for the selected IP Address. This view is useful for obtaining a summary of the IP address status so that you can better determine any patterns in behavior and activity.</p> <p>Click the  Open icon to view more information about a specific status.</p>


## IP Address Form: Conclusions Tab

The ["IP Address Form" \(on page 73\)](#) provides details about the selected IP address .

For information about each tab:

### Conclusions Table

Attribute	Description
Outstanding Status Conclusions	<p>The dynamically generated list of summary statuses of the IP address at points in time that contributed to the current overall status of the selected IP address. Status is set by the Causal Engine.</p> <p>Each conclusion listed is still outstanding and applies to the current overall status.</p> <p>This view is useful for obtaining a quick summary of the status and problem description for the current node's interfaces that led up to the node's most current status.</p>

Attribute	Description
	<p>Examples of conclusions that might appear together are listed below:</p> <ul style="list-style-type: none"> <li>• SNMP Agent Not Responding</li> <li>• Interface Down</li> <li>• Address Down</li> </ul> <p>The status value is correlated based on the most critical conclusions. Click the  Open icon to view more information about a specific conclusion.</p>

## IP Address Form: Capabilities Tab

The ["IP Address Form" \(on page 73\)](#) provides details about the selected IP address.

### For information about each tab:

The IP Address Form: Capabilities tab displays a table view of any capabilities added to the IP Address object by NNMi or an external application. For example, NNMi uses the capability feature to identify an **Anycast Rendezvous Point IP Address**<sup>1</sup> so it is not polled. NNMi assigns the Anycast Rendezvous Point IP address the following capability: `com.hp.nnm.capability.address.anycast`.

**Note:** Because the values are generated by NNMi or an external application, Capability values cannot be modified.

### Capabilities Table

Attribute	Description
Capability	<p>The name of the capability added to an IP address object by either NNMi or an external application. For more information, see:</p> <ul style="list-style-type: none"> <li>• <a href="#">"IP Address Capability Form" (on page 78)</a></li> <li>• <a href="#">"IP Address Capabilities Provided by NNMi" (on page 77)</a></li> </ul>
Unique Key	<p>The database identifier for the capability that either NNMi or an external application added to this interface.</p> <p><b>Note:</b> Capabilities added by NNMi use a Unique Key value that begins with the prefix: <code>com.hp.nnm.capability</code>. See <a href="#">"IP Address Capabilities Provided by NNMi" (on page 77)</a> for a description of the capabilities provided by NNMi that might appear under the IP Address Form: Capabilities Tab.</p>

## IP Address Capabilities Provided by NNMi

The IP Address Form: Capabilities Tab displays a table view of any capabilities that have been added to the IP Address object. Capabilities that begin with `com.hp.nnm.capability` represent capabilities that NNMi provides. External applications can also add capabilities for patterns, multi-cast network configurations, and other objects.

## NNMi IP Address Capabilities

Capability	Unique Key	Description
loopback	<code>com.hp.nnm.capability.address.loopback</code>	Used to identify a <b>loopback address</b> <sup>1</sup> .
anycast	<code>com.hp.nnm.capability.address.anycast</code>	Used to identify a loopback address that is an <b>Anycast Rendezvous Point IP Address</b> <sup>2</sup> .  Anycast Rendezvous Point IP Addresses are loopback addresses used for routers in multi-cast network configurations. These duplicate IP addresses are excluded from monitoring.

## IP Address Capability Form

This form describes a capability added to the IP address object by NNMi or an external application. For example, NNMi uses the capability feature to identify an **Anycast Rendezvous Point IP Address**<sup>3</sup>. To help identify the Anycast Rendezvous Point IP addresses so they are not polled, NNMi assigns the IP address the following capability:`com.hp.nnm.capability.address.anycast`.

**Note:** Because the values are generated by NNMi or an external application, Capability values cannot be modified.

Each Capability attribute is described in the table below.

### Basics Attributes

Attribute	Description
Capability	Label used to identify the Capability that was added to the IP address object. The Capability value is listed in the table on the Capabilities tab in an IP Address form. See <a href="#">"IP Address Capability Form" (on page 78)</a> .
Unique Key	Used as a unique identifier for the Capability. Any capability provided by NNMi begins with the prefix <code>com.hp.nnm.capability</code> .  <b>Note:</b> Capabilities added by NNMi use a Unique Key value that begins with the prefix: <code>com.hp.nnm.capability</code> . See <a href="#">"IP Address Capabilities Provided by NNMi" (on page 77)</a> for a description of the capabilities provided by NNMi that might appear under the IP Address Form: Capabilities Tab.

## IP Address Form: Registration Tab

The ["IP Address Form" \(on page 73\)](#) provides details about the selected IP address .

<sup>1</sup>The address associated with the loopback interface. The loopback interface is a virtual interface on a device that provides a route for internal communication. Many vendors provide a specially configured loopback for management purposes. Exact details of how loopbacks are configured varies by vendor and model. See each device's documentation for details. NNMi identifies these loopback addresses by using IfType 24, softwareloopback from the IANA ifType-MIB.

<sup>2</sup>Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

<sup>3</sup>Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

For information about each tab:

### Registration






Attribute	Description
Created	Date and time the selected object instance was created. NNM uses the locale of the client and the date and time from the NNMi management server.
Last Modified	Date the selected object instance was last modified. NNM uses the locale of the client and the date and time from the NNMi management server.

## Router Redundancy Group Form (NNMi Advanced)

The Router Redundancy Group Form provides details about the Router Redundancy Group selected. This form is useful for troubleshooting purposes. You can access information about the name, status, and Router Redundancy Members (routers) associated with this Router Redundancy Group.

For information about each tab:

### Basics Attributes

Attribute	Description
Name	The name assigned to this Router Redundancy Group. This name is the virtual IP address protected by this group and used by the router that is actively routing information packets (for example, HSRP Active or VRRP Master).
Status	<p>Router Redundancy Group Status reflects the most serious Severity value of the incidents associated with the Router Redundancy Group. Possible values are:</p> <ul style="list-style-type: none"> <li> Normal</li> <li> Warning</li> <li> Minor</li> <li> Major</li> <li> Critical</li> </ul> <p>See <a href="#">"Watch Status Colors" (on page 129)</a> for more information about Severity values.</p> <p><b>Note:</b> The icons are displayed only in table views.</p>
Group Number	The group number that was configured for the current Router Redundancy Group.
Number of Members	Specifies the number of members that belong to the current Router Redundancy Group.

### Related Topics

["Router Redundancy Group View \(NNMi Advanced\)" \(on page 24\)](#)

["Non-Normal Router Redundancy Group View \(NNMi Advanced\)" \(on page 123\)](#)

["Router Redundancy Member Form \(NNMi Advanced\)" \(on page 80\)](#)

## Router Redundancy Group Form: Router Redundancy Members Tab (NNMi Advanced)


The table on this tab lists all routers and the associated interface that currently belong to the Redundancy Router Group. The ["Router Redundancy Group Form \(NNMi Advanced\)" \(on page 79\)](#) provides details about the selected Router Redundancy Group.

For information about each tab:

### Router Redundancy Members Table

Attribute	Description
Current State	The current HSRP or VRRP state for the selected Router Redundancy Group Member. See <a href="#">"Router Redundancy Member Form (NNMi Advanced)" (on page 80)</a> for more information about the possible state values.
Previous State	The previous HSRP or VRRP state for the selected Router Redundancy Group Member. See <a href="#">"Router Redundancy Member Form (NNMi Advanced)" (on page 80)</a> for more information about the possible state values.
Priority	Number used to rank the Router Redundancy Members. The member with the numerically higher priority becomes the Active (HSRP) or Master (VRRP).
Hosted On Node	Name of the selected router that is a member of the current Router Redundancy Group. The name is the hostname assigned to the router. See <a href="#">"Node Form" (on page 28)</a> for more information about node names.
Redundancy Interface	The interface that is being used by the router to participate in the Router Redundancy Group.

To see more details about a particular Router Redundancy Member:

Click the  Open icon that precedes the Router Redundancy Member of interest to open the ["Router Redundancy Group Form \(NNMi Advanced\)" \(on page 79\)](#).

## Router Redundancy Member Form (NNMi Advanced)

The Router Redundancy Member form provides details about a router in the Router Redundancy Group.




This form is useful for troubleshooting purposes. You can access information about the router name and status, as well as conclusions information to assist you in understanding the router's HSRP or VRRP state. You can also see the name of each tracked object associated with the router. A tracked object represents the interface responsible for delivering the outbound information packet that was originally sent to the current Router Redundancy Member.















For information about each tab:

### Basics Attributes

Attribute	Description
Name	Name of the selected router and its associated interface that is a member of the current Router Redundancy Group.



Attribute	Description
	<p><b>Note:</b> NNMi determines this Name value.</p> <p>The name includes the fully qualified DNS name assigned to the router and the Name assigned to the interface.</p> <p>This name appears in the following format:</p> <p><i>&lt;fully qualified hostname assigned to the router&gt;[Interface Name:group_number]</i></p> <p>For example: HSRPRouter1.xyz.ab.com[Se1/1:1]</p> <p>See <a href="#">"Node Form" (on page 28)</a> for more information about node names.</p>
Redundancy Interface	<p>The interface that is being used by the router to participate in the Router Redundancy Group.</p> <p>To find out more information about this interface:</p> <p>Click the  Lookup icon and choose one of the following options:</p> <ul style="list-style-type: none"><li>•  Quick View to view a summary of the interface details.</li><li>•  Open to open the interface form.</li></ul>

Attribute	Description
Current State	<p>HSRP or VRRP State of the Router Redundancy Member. Possible states for routers using the HSRP or VRRP protocol are listed below.</p> <p><b>HSRP States</b></p> <ul style="list-style-type: none"> <li> <b>Active</b> - Indicates the router is forwarding packets that are sent to the router redundancy group.</li> <li> <b>Initial</b> - Indicates HSRP is not running. This state occurs when an interface first comes up.</li> <li> <b>Learn</b> - Indicates the router has not yet determined the virtual IP address. This state occurs when the router is waiting to hear from the active router.</li> <li> <b>Listen</b> - Indicates the router knows the virtual IP address, but it is neither the active or standby router. In this state, the router is waiting for a message from the active and standby routers.</li> <li> <b>Speak</b> - Indicates the router knows the virtual IP address. In this state, the router sends periodic messages and is ready to become an active or standby router.</li> <li> <b>Standby</b> - Indicates the router is a candidate to become the next active router.</li> </ul> <p><b>VRRP States</b></p> <ul style="list-style-type: none"> <li> <b>Initialize</b> - Indicates the router is not running VRRP. This state occurs when an interface first comes up.</li> <li> <b>Master</b> - Indicates the router is forwarding packets that are sent to the router redundancy group.</li> <li> <b>Backup</b> - Indicates the router is a candidate to become the next master router.</li> </ul> <p>If NNMi is unable to poll the interface used to identify the selected router in the Router Redundancy Group, one of the following states is set for the selected router's interface:</p> <ul style="list-style-type: none"> <li> <b>Agent Error</b> – Indicates an SNMP error was returned in response to an SNMP query to the interface's SNMP agent.</li> <li> <b>Other</b> – The SNMP agent on the interface responded with a value for the MIB variable used to determine the Router Redundancy Member State that is not recognized.</li> <li> <b>No Polling Policy</b> – Indicates that the interface is not included in any internal NNMi polling policies, and therefore not polled for the information.</li> <li> <b>Not Polled</b> – Indicates that the interface is intentionally not polled, based on current Monitoring Configuration settings, current Communication Configuration settings, or because the parent Node is set to Not Managed or Out of Service.</li> <li> <b>Unavailable</b> – The SNMP agent on the interface responded, but returned a null value for the request to the MIB variable used to determine the Router Redundancy Member State.</li> </ul>
Previous State	The previous HSRP or VRRP State of the Router Redundancy Member. Possible values are described under <a href="#">Current State</a> .
Priority	Number used to rank the Router Redundancy Members. The member with the numerically higher priority becomes the Active (HSRP) or Master (VRRP).

Attribute	Description
-----------	-------------

### Router Redundancy Member Form: Tracked Objects Tab (NNMi Advanced)

A tracked object is the outbound interface responsible for delivering the outbound information packet that was originally sent to a selected inbound interface on a router that is part of the Router Redundancy Group. A Router Redundancy Member can have one or more associated tracked objects

The "[Router Redundancy Member Form \(NNMi Advanced\)](#)" (on page 80) provides details about the selected Router Redundancy Member. Each Router Redundancy Member is a router in the Router Redundancy Group.

For information about each tab:




#### Tracked Objects Table

Attribute	Description
Track Priority	<p>Number used to rank the tracked object. This number is used indirectly in the calculation that determines the next Active or Master member of the Router Redundancy Group whenever a State change occurs.</p> <p>When a tracked object goes down, the priority of the tracked object (Track Priority) is subtracted from its Router Redundancy Member Priority value to produce a smaller member Priority number. If this new Priority number is smaller than one of the other member Priority numbers, the member with the highest Priority value becomes the new Master or Active router in the current Router Redundancy Group.</p> <p>For example, if an interface whose Track Priority is 20 goes down on a Router Redundancy Member whose member Priority is 250:</p> <ul style="list-style-type: none"> <li>The Track Priority (20) is subtracted from its member Priority (250-20=230).</li> <li>The new member Priority (230) is then compared to the Priority value of the other members in the Router Redundancy Group.</li> <li>If one of the members in the Router Redundancy Group has a higher member Priority, for example, 240, that member becomes the Active or Master router in the group.</li> </ul>
Name	<p>Name of the selected router and its associated interface that is a member of the current Router Redundancy Group.</p> <p><b>Note:</b> NNMi determines this Name value.</p> <p>The name includes the fully qualified DNS name assigned to the router and the name assigned to the interface.</p> <p>See "<a href="#">Tracked Objects Form (NNMi Advanced)</a>" (on page 84) for more information about tracked objects.</p> <p>This name appears in the following format:</p> <p><i>&lt;fully qualified hostname assigned to the router&gt;[Interface Name]</i></p> <p>For example: HSRPRouter1.xyz.ab.com[Se1/1]</p> <p>See "<a href="#">Node Form</a>" (on page 28) for more information about node names.</p>

### Tracked Objects Form (NNMi Advanced)

Your network administrator might have set up groups of redundant routers to help ensure that information packets reach their intended destination. A tracked object is the outbound interface responsible for delivering the outbound information packet that was originally sent to a selected inbound interface on a router that is part of the Router Redundancy Group. A Router Redundancy Member can have one or more associated tracked objects.

#### Basics Attributes

Attribute	Description
Tracked Object	<p>Name used to identify the selected tracked object. The name includes the fully-qualified DNS name assigned to the router and the name assigned to its associated tracked object .</p> <p>This name appears in the following format:</p> <p><i>&lt;fully qualified hostname assigned to the router&gt;[Interface Name]</i></p> <p>For example: HSRPRouter1.xyz.ab.com[Se1/1]</p> <p>To find out more information about this interface:</p> <p>Click the  Lookup icon and choose one of the following options:</p> <ul style="list-style-type: none"><li> Quick View to view a summary of the interface details.</li><li> Open to open the Interface form.</li></ul>
Track Priority	<p>Number used to rank the tracked object. This number is used indirectly in the calculation that determines the next Active or Master member of the Router Redundancy Group whenever a State change occurs.</p> <p>When a tracked object goes down, the priority of the tracked object (Track Priority) is subtracted from its Router Redundancy Member Priority value to produce a smaller member Priority number. If this new Priority number is smaller than one of the other member Priority numbers, the member with the highest Priority value becomes the new Master or Active router in the current Router Redundancy Group.</p> <p>For example, if an interface whose Track Priority is 20 goes down on a Router Redundancy Member whose member Priority is 250:</p> <ul style="list-style-type: none"><li>The Track Priority (20) is subtracted from its member Priority (250-20=230).</li><li>The new member Priority (230) is then compared to the Priority value of the other members in the Router Redundancy Group.</li><li>If one of the members in the Router Redundancy Group has a higher member Priority, for example, 240, that member becomes the Active or Master router in the group.</li></ul>

### Router Redundancy Group Form: Virtual IP Addresses Tab (NNMi Advanced )

**Tip:** See "[IP Address Form](#)" (on page 73) for an explanation of the columns in the Virtual IP Addresses table view.

The "[Router Redundancy Group Form \(NNMi Advanced\)](#)" (on page 79) provides details about the selected Router Redundancy Group.


**For information about each tab:**

## Virtual IP Addresses Table View

### Description

The Virtual IP addresses Tab displays a table view of the virtual IP addresses associated with the selected Router Redundancy Group. The virtual IP address is the IP address protected by this group and used by any router that is actively routing information packets (for example, HSRP Active or VRRP Master). For each virtual IP address displayed, you can see the IP address value.

To see more information about a specific IP address:

1. Select the IP address of interest by checking the  selection box that precedes the object information.
2. Click the  Open icon to open the ["IP Address Form" \(on page 73\)](#) and view more information about the specific IP address.

## Virtual IP addresses Form (NNMi Advanced)

A virtual IP address is an address protected by the Router Redundancy Group and used by the router that is actively routing information packed (for example, HSRP Active or VRRP Master).

Basic Attributes

### Virtual IP Addresses

Attribute	Description
Value	IP address value for the virtual IP address.

## Router Redundancy Group Form: Incidents Tab (NNMi Advanced)

**Tip:** See ["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in the incident view's column headings.

The ["Router Redundancy Group Form \(NNMi Advanced\)" \(on page 79\)](#) provides details about the selected Router Redundancy Group.


**For information about each tab:**

### Incidents Table

#### Description

Table view of the incidents associated with the selected Router Redundancy Group. These incidents are sorted by creation time so that you can view the incidents in chronological order. Use this view to determine which incidents are still open for the selected Router Redundancy Group.

To see more information about an incident:

1. Select the incident of interest by checking the  selection box that precedes the object information.
2. Click the  Open icon to open the ["Incident Form" \(on page 134\)](#) and view more information about a specific incident.

## VLAN Form

The VLAN form provides details about the selected virtual local area network, and lists all ports known to participate in this VLAN.

**Note:** A trunk port can participate in multiple VLANs.

**For information about each tab:**

### Basic Attributes

Attribute	Description
VLAN Id	The identification value for the current VLAN. This value is taken directly from the MIB file provided by the Vendor.
Name	The name value from the MIB provided by the Vendor. If no name is provided in the MIB file, the same string as the VLAN Id is used.
Member Node [Interface]	<p>NNMi selects a representative Member Node and Member Interface for the current VLAN. These members help to distinguish VLANs that use the same identification number.</p> <p>NNMi selects the Member Node using the following criteria:</p> <ul style="list-style-type: none"><li>• The node is a member of the VLAN.</li><li>• The node has the lexicographically ordered first node hostname.</li></ul> <p>NNMi selects the Member Interface using the following criteria:</p> <ul style="list-style-type: none"><li>• The interface must be on the Member Node.</li><li>• The interface is a member of the VLAN.</li><li>• The interface has the lexicographically ordered first interface name.</li></ul>
Member Node Count	Specifies the number of nodes that belong to the current VLAN.

### Related Topics:


["VLANs View \(Inventory\)" \(on page 20\)](#)

## VLAN Form: Ports Tab

**Note:** A trunk port can participate in multiple VLANs.

The "[VLAN Form](#)" (on page 86) provides details about the selected VLAN.

### Ports Associated with this VLAN

Attribute	Description
Ports	<p>Table view of the ports associated with the selected VLAN. Use this table to access information about each port associated with the selected VLAN across all member devices.</p> <p>Click the  Open icon to open the "<a href="#">Port Form</a>" (on page 87) and view more information about a port.</p>

**Related Topics:**







["VLANs View \(Inventory\)" \(on page 20\)](#)

## Port Form

The Port form provides details about the port you selected on the Node form or VLAN form. The following table describes the fields included on the Port form.

**For information about each tab:**

**Basic Attributes**

Attribute	Description
Name	The port name consists of <Card-number / Port-number>.
Hosted on Node	Node on which the port resides. This is the current value in NNMi's database for the Name attribute of the host device. The value could be a DNS name, a MIB II sysName, or an address (depending on how your NNMi administrator configured the discovery process).  Click the  Lookup icon and select  Quick View or  Open to display more information about the node.
Associated Interface	The current value from the Name attribute on the Interface form. The most accurate interface name available to the initial discovery process: IF MIB ifName, ifAlias, or ifType+ifIndex values.  Click the  Lookup icon and select  Quick View or  Open to display more information about the interface.

**Related Topics:**

["Node Form" \(on page 28\)](#)


["VLAN Form" \(on page 86\)](#)

## Port Form: VLANs Tab

The Port form provides details about the port you selected on the Node form or VLAN form. The following table describes the fields included on the Port form.

The ["Port Form" \(on page 87\)](#) provides details about the selected VLAN.

**VLANs Attributes**

Attribute	Description
VLANs	Table view of the VLANs to which the selected port belongs. You can use this table to determine the VLAN ID number and name for each VLAN associated with the selected port.  Click the  Open icon to open the <a href="#">"VLAN Form" (on page 86)</a> and view more information about a specific VLAN.

**Related Topics:**

["Node Form" \(on page 28\)](#)

["VLAN Form" \(on page 86\)](#)

## Node Group Form

**Note:** Island Node Groups are a special kind of Node Group that NNMi manages internally. Therefore, NNMi administrators should not modify Island Node Group configurations. NNMi overrides any user changes the next time NNMi updates the Island Node Group discovery information. See "Help for Administrators" for more information about Island Node Groups.

Membership in each node group is determined by a number of factors specified on the Node Group form. The NNMi administrator can create and modify Node Group definitions. The NNMi administrator can also configure Node Groups as filters in table views. NNMi monitors the status of each Node Group over time. NNMi also provides a map of each Node Group.

Each node group includes one or more of the following:

- Device Filters (by any combination of category, vendor, family, profile)
- Additional Filters
- Additional Nodes (specific nodes identified by Hostname)

If Device Filters and Additional Filters are in use, nodes must match *both* the Device Filters and the Additional Filters specifications to belong to this Node Group. Nodes that are specified as Additional Nodes are *always* included in the Node Group.

**For information about each tab:**

**Tip:** [Special Actions are available](#) within the Node Group view and Interface Group view.

Depending on your role, you can use Node Groups in several ways:

### Node Group Basic Settings

Attribute	Description
Name	The name of this group (text string specified by the NNMi administrator).
Status	Overall status for the specified node group. NNMi follows the ISO standard for status classification. See the <a href="#">"Node Group Form: Status Tab" (on page 93)</a> for more information.
Add to View Filter List	If disabled <input type="checkbox"/> , this node group does not appear in any node group filter lists for node, interface, IP address, and incident views. If enabled <input checked="" type="checkbox"/> , this node group is available as a filter for all node, interface, IP address, and incident views.
Notes	<i>Optional.</i> If your role allows, enter any information that might be useful to you and your team.  Type a maximum of 1024 characters. Alpha-numeric, spaces, and special characters (~ ! @ # \$ % ^ & * ( ) _ +) are allowed.

### Node Group Settings (NNM iSPI Performance)

Attribute	Description
Add to Filter List	(NNM iSPI Performance) Using this feature is entirely optional. The NNM iSPI Performance software, such as NNM iSPI Performance for Metrics or NNM iSPI Performance for Traffic, can monitor your network without any exported filter.



Attribute	Description
	<p>Enable only for groups that are needed as filters in NNM iSPI Performance reports. It may take up to an hour before the results are visible in the NNM iSPI Performance reports. Choose wisely because establishing a filter requires significant NNM iSPI Performance software processing time.</p> <p>If disabled <input type="checkbox"/>, this group is not available as a filter in NNM iSPI Performance reports.</p> <p>If enabled <input checked="" type="checkbox"/>, this group appears in the Optional Filters selection panel of the NNM iSPI Performance reports.</p>

## Node Group Form: Device Filters Tab

*Optional:* Determine Node Group members by vendor, family, model, or other device characteristics such as SNMP object identifiers.


If any hostname wildcards or device filters are in use:

- By default, when the hostname wildcard or device filter list is empty, no nodes match the criteria. To match all nodes, use the \* (asterisk) wildcard.
- When either or both hostname wildcard and device filters are enabled, nodes must match ALL specifications to belong to this node group.

The "[Node Group Form](#)" (on page 88) provides details about the selected node group.

For information about each tab:

### Device-Characteristic Filters Table

Attribute	Description
Device Filter	<p>Table view of the device category, vendor, product family, or product model filters associated with the selected node group.</p> <p>Click the  Open icon to open the "<a href="#">Node Device Filter Form</a>" (on page 89) and view more information about a filter specification.</p>

## Node Device Filter Form





*Optional:* Node Group definitions can specify membership by device vendor, family, model, or SNMP object identifiers.

When using node Device Filters, note the following:

- If Device Filters and Additional Filters are in use, nodes must match *both* the Device Filters and the Additional Filters specifications to belong to this Node Group.
- Nodes that are specified as Additional Nodes *always* pass any filters.

### Device Attribute Filters Table

Attribute	Description
Device Category	<i>Optional:</i> A particular category of devices. The drop-down list displays all available choices.
Device Vendor	<i>Optional:</i> A particular vendor. The drop-down list displays all available choices.

Attribute	Description
Device Category	<i>Optional:</i> A particular category of devices. The drop-down list displays all available choices.
Device Family	<i>Optional:</i> A particular family of devices. To see all available choices, click the  Open icon and use the  Quick Find icon.
Device Profile	<i>Optional:</i> A particular device model or SNMP object ID. To see all available choices, click the  Open icon and use the  Quick Find icon.

## Node Group Form: Additional Filters Tab

**Tip:** If you are an NNMi Administrator, see the "Help for Administrators" for more information about how to use the Additional Filters Editor.

The Additional Filters tab enables the NNMi administrator to use expressions to further define which nodes to include in a Node Group.

If any Additional Filters are created:

- NNMi first evaluates any hostname filters and device filters. Nodes must match *at least one* specification to belong to this Node Group.
- NNMi then evaluates any Additional Filter expression. Nodes *must also match all* Additional Filters expression specifications to belong to this Node Group.

The "[Node Group Form](#)" (on page 88) provides details about the selected Node Group.

### For information about each tab:

If an NNMi administrator created any Additional Filters for the selected Node Group, NNMi displays the Additional Filters expression.

## Node Group Form: Additional Nodes Tab


*Optional:* Determine Node Group members by specifying each device hostname (or address when hostname is not available).

Nodes that are specifically listed are *always* included in this node group.

The "[Node Group Form](#)" (on page 88) provides details about the selected node group.

### For information about each tab:

#### Specific-Device Filters Table

Attribute	Description
Node Hostname	Table view of the hostnames for the additional nodes added to the selected Node Group. <b>Note:</b> NNMi always converts hostnames to all lowercase.  Click the  Open icon to open the " <a href="#">Additional Node Form</a> " (on page 91) and view more information about a filter specification.

## Additional Node Form

*Optional:* Node Group definitions can identify specific devices by hostname (or address when hostname is not available).

Nodes that are specified as Additional Nodes are *always* included in the Node Group.

The "[Node Group Form](#)" (on page 88) provides details about the selected Node Group.

## Specific Device Filter

Attribute	Description
Node Hostname	<p>The Hostname attribute value on the Node form of the discovered node must match what is entered here (see the Hostname attribute the "<a href="#">Node Form</a>" (on page 28) for more information).</p> <p><b>Note:</b> NNMi always converts hostnames to all lowercase.</p> <p>If a device has multiple hostnames or no hostname, NNMi follows a set of rules to determine the hostname. Click here for details.</p> <ol style="list-style-type: none"> <li>1. If a hostname is available, it must resolve to a valid IP address. NNMi stores the fully-qualifiedhostname in the database as all lowercase characters.</li> <li>2. If more than one address is associated with a node, the <b>loopback address</b><sup>1</sup> is used with the following exceptions:                         <ul style="list-style-type: none"> <li>■ NNMi prefers loopback interfaces for management communication, where possible. However, NNMi automatically filters out addresses in the reserved loopback network range 127/24 (127.*.*).</li> <li>■ NNMi ignores any address that is virtual (HSRP/VRRP) or an <b>Anycast Rendezvous Point IP Address</b><sup>2</sup>.</li> </ul> </li> <li>3. If a node has multiple loopback addresses, NNMi uses the loopback address with the lowest number that resolves to a hostname (for example, 10.16.42.197 is a lower number than 10.16.197.42).</li> <li>4. If no loopback address resolves to a hostname and the device supports SNMP, NNMi uses the current value from the Management Address attribute on the Node form.</li> <li>5. If the device does not support SNMP, the IP address or DNS name found during the current rediscovery cycle is used as the hostname.</li> </ol> <p>This sequence is repeated during each rediscovery cycle. The hostname could change from cycle to cycle (for example, if an address did not respond to SNMP queries due to network problems or node reconfiguration).</p>

---

<sup>1</sup>The address associated with the loopback interface. The loopback interface is a virtual interface on a device that provides a route for internal communication. Many vendors provide a specially configured loopback for management purposes. Exact details of how loopbacks are configured varies by vendor and model. See each device's documentation for details. NNMi identifies these loopback addresses by using IfType 24, softwareloopback from the IANA ifType-MIB.

<sup>2</sup>Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

## Node Group Form: Child Node Groups Tab

The ["Node Group Form" \(on page 88\)](#) provides details about the selected Node Group.

Child Node Groups can be created to associate groups of nodes in a hierarchy. For example, a hierarchical set of Node Groups might be based on geographical location. The Parent Node Group might be named **United States** to represent all of the nodes in the United States. Additional Node Groups might exist for each state in which your business offices reside (for example **Colorado** and **California**). Each of these individual state Node Groups are added as Child Node Group of the **United States** Node Group.

For information about each of the columns displayed in the Child Node Groups table, see ["Node Group Hierarchy \(Child Node Group\) Form" \(on page 92\)](#).

By default, each Child Node Group is represented by a hexagon that appears with the other Node objects of the Parent Node Group in the Node Group Map. Child Node Group objects can be moved and have their locations saved with other Node objects in the map. Unlike other Node objects, double-clicking a Child Node Group object displays a map of the nodes in the Child Node Group rather than the object's form.

An NNMi administrator alternatively can configure the map to display all nodes in a Child Node Group as though its contents are directly in the Parent Node Group by setting the **Expand Child in Parent Node Group Map** attribute. An NNMi administrator must set this option for each Child Node Group that should be expanded. See ["Node Group Hierarchy \(Child Node Group\) Form" \(on page 92\)](#) for more information.

**For information about each tab:**

### Related Topics

["Node Group Maps" \(on page 99\)](#)

["Navigating within a Node Group Map" \(on page 100\)](#)

["Position Nodes on a Node Group Map" \(on page 101\)](#)

## Node Group Hierarchy (Child Node Group) Form

Child Node Groups associate groups of nodes in a hierarchical order. For example, the Parent Node Group might be named **United States** to represent all of the nodes in the United States. Additional Node Groups might exist for each state in which your business offices reside (for example **Colorado** and **California**). Each of these individual state Node Groups can be a Child Node Group of the **United States** Node Group.

The following table describes each of the **Basics** attributes in the **Node Group Hierarchy** form.

### Basics Attributes

Attribute	Description
Child Node Group	Indicates the name of a Node Group that is below the current Node Group in the hierarchical order. For example, <b>Colorado</b> could be a Child Node Group to a Node Group named <b>United States</b> .  <b>Note:</b> This attribute appears as the <b>Name</b> column in the <b>Child Node Groups</b> table view.
Expand Child in Parent Node Group Map	Used to indicate whether all of the nodes contained in a Child Node Group are displayed in the Node Group Map as though they were directly contained in the parent node group.  If enabled, each node in the group appears as a separate node on the Node Group Map.

Attribute	Description
Child Node Group	<p>Indicates the name of a Node Group that is below the current Node Group in the hierarchical order. For example, <b>Colorado</b> could be a Child Node Group to a Node Group named <b>United States</b>.</p> <p><b>Note:</b> This attribute appears as the <b>Name</b> column in the <b>Child Node Groups</b> table view.</p> <hr/> <p>If disabled, a single object represents a Child Node Group on the Node Group Map.</p> <p>Note the following:</p> <ul style="list-style-type: none"> <li>• If the current Node Group has one or more Child Node Groups, each Child Node Group is also displayed. Child Node Groups are indicated using a hexagon as shown below:                             <ul style="list-style-type: none"> <li>■</li> </ul> </li> <li>• If any Child Node Group is a parent to other Child Node Groups, those Child Node Groups are also displayed on the map as follows:                             <ul style="list-style-type: none"> <li>■ If the Child Node Group has the <b>Expand Child in Parent Node Group Map</b> attribute disabled, the Child Node Group appears as a hexagon.</li> <li>■ If any Child Node Group has the <b>Expand Child in Parent Node Group Map</b> attribute enabled, NNMi displays each of the nodes in that Child Node Group.</li> </ul> </li> </ul> <p><b>Note:</b> This attribute appears in the <b>ECiNM</b> column in the <b>Child Node Groups</b> table view.</p>

**Related Topics**

["Node Group Maps" \(on page 99\)](#)

["Position Nodes on a Node Group Map" \(on page 101\)](#)



**Node Group Form: Status Tab**









The Node Group status is calculated based on the status of the nodes within the group.

The ["Node Group Form" \(on page 88\)](#) provides details about the selected Node Group.

**For information about each tab:**

**Status Attributes**

Attribute	Description  <b>Minor — At least 20 percent of the nodes in the Node Group have a Status of Minor.</b>
Status	<p>The Node Group status is calculated based on the status of the nodes within the group. NNMi follows the ISO standard for status classification. Possible values are:</p> <p><b>Note:</b> Your NNMi administrator can configure how a Node Group Status is calculated. The percentages listed below represent the default percentages, which might have been changed. By default, NNMi sets up the Node Group status so that it is equal to the most severe Status of any node in the Node Group. See "Help for Administrators" for more information.</p> <ul style="list-style-type: none"> <li> <b>No Status</b> — The Node Group has just been added and NNMi has not yet calculated the status.</li> </ul>

Attribute	Description  <b>Minor</b> — At least 20 percent of the nodes in the Node Group have a Status of <b>Minor</b> .
	<p> <b>Normal</b> — All nodes in the Node Group have a status of Normal or the threshold specified for this Target Status has not been reached.</p> <p> <b>Unknown</b> — All nodes within the Node Group have a status of <b>Unknown</b>.</p> <p> <b>Warning</b> — At least 30 percent of the nodes within the Node Group have a status of <b>Warning</b>.</p> <p> <b>Minor</b> — At least 20 percent of the nodes in the Node Group have a Status of <b>Minor</b>.</p> <p> <b>Major</b> — At least 10 percent of the nodes within the Node Group have a status of <b>Major</b>.</p> <p> <b>Critical</b> — At least 5 percent of the nodes in the group have a status of <b>Critical</b>.</p> <p><b>Note:</b> When the percentages for more than one Status has been exceeded, NNMi propagates the most severe status. For example, if 40 percent of the nodes in a Node Group are in Warning Status and 30 percent are in Minor Status, NNMi assigns the Node Group a Status of Minor.</p> <p>See "<a href="#">Watch Status Colors</a>" (on page 129) for more information about possible status values.</p> <p><b>Note:</b> The icons are displayed only in table views.</p>
Status Last Modified	Date and time indicating when the status was last set.
Status History	List of up to the last 30 changes in status for the selected node. This view is useful for obtaining a summary of the node group status so that you can better determine any patterns in behavior and activity.
	Click the  Open icon to view more information about a specific status.

## Interface Group Form

Each interface group can include one or more interface-type specifications (based on industry-standard IANA ifType-MIB variables). The NNMi administrator can create and modify interface group definitions. The NNMi administrator can also configure interface groups as filters in table views.

### For information about each tab:

**Tip:** [Special Actions are available](#) within the Node Group and Interface Group views.

Depending on your role, Interface Groups can be used in several ways:

### Interface Group Basics

Attribute	Description
Name	The name of this group (text string specified by the NNMi administrator).
Add to View Filter List	<p>If disabled <input type="checkbox"/>, this interface group does not appear in any interface group filter lists for interface and IP address views.</p> <p>If enabled <input checked="" type="checkbox"/>, this interface group is a filter for all interface and IP address views.</p>

Attribute	Description
Node Group	<i>Optional.</i> If configured, this Interface Group is associated with a Node Group and serves as a filter for that Node Group.
Notes	<i>Optional.</i> If your role allows, enter any information that might be useful to you and your team.  Type a maximum of 1024 characters. Alpha-numeric, spaces, and special characters (~ ! @ # \$ % ^ & * ( ) _ +) are allowed.

### Interface Group Settings (NNM iSPI Performance)

Attribute	Description
Add to Filter List	<p>(NNM iSPI Performance) Using this feature is entirely optional. The NNM iSPI Performance software, such as NNM iSPI Performance for Metrics or NNM iSPI Performance for Traffic, can monitor your network without any exported filter.</p> <p>Enable only for groups that are needed as filters in NNM iSPI Performance reports. It may take up to an hour before the results are visible in the NNM iSPI Performance reports. Choose wisely because establishing a filter requires significant NNM iSPI Performance software processing time.</p> <p>If disabled <input type="checkbox"/>, this group is not available as a filter in NNM iSPI Performance reports.</p> <p>If enabled <input checked="" type="checkbox"/>, this group appears in the Optional Filters selection panel of the NNM iSPI Performance reports.</p>

### Interface Group Form: IfType Filters Tab


Interface Group members are filtered by industry-standard IANA ifType-MIB variables.

**Note:** To be included in this Interface Group, interfaces must match *ALL* criteria listed on this tab.

The "[Interface Group Form](#)" (on page 94) provides details about the selected interface group.

**For information about each tab:**



#### IfType Filters Table

Attribute	Description
IfType Filters	<p>Table view of all IfType filters associated with the selected interface group.</p> <p>Click the  Open icon to open the "<a href="#">IfType Filter Form</a>" (on page 95) and view more information about a filter specification.</p>

#### IfType Filter Form

Displays the specification of the selected interface-type filter. This filter is based on an industry-standard IANA ifType-MIB variable.

## IfType Specification






Attribute	Description
IfType	<p>Click the  Lookup icon and select  Open to display the "<a href="#">IfType (Interface Type) Form</a>" (on page 96) and view more information about the specified IANA ifType-MIB variable.</p> <p>If your role allows, you can easily choose from a list of all known industry-standard IANAif-Type-MIB variables (as of the time NNMi was released). You can also add a new value. (For more information, see <a href="http://www.iana.org/assignments/ianaiftype-mib">http://www.iana.org/assignments/ianaiftype-mib</a>)</p>

## IfType (Interface Type) Form

Displays information about the selected industry-standard IANA ifType-MIB variable.

The NNMi administrator can change these settings.

### Interface Type Definition

Attribute	Description
IfType	<p>Text string. The IANA ifType TEXTUAL-CONVENTION values extracted from the IANA ifType-MIB. This text string displays as the Interface Type attribute value in Interfaces views. (For more information, see <a href="http://www.iana.org/assignments/ianaiftype-mib">http://www.iana.org/assignments/ianaiftype-mib</a>.)</p> <p>If your role allows, click the  Lookup icon and select one of the options from the drop-down menu:</p> <ul style="list-style-type: none"><li> Quick View to display summary information for the currently selected IfType.</li><li> Quick Find to view and select from the list of all existing IfTypes.</li><li> Open to display the details of the currently selected IfType.</li><li> New to create a new SNMPv3 Setting.</li></ul>
Number	Industry-standard number assigned to this ifType.
Description	<p><i>Optional.</i> If your role allows, provide any description that would be useful for communication purposes within your team.</p> <p>Type a maximum of 2048 characters. Alpha-numeric, punctuation, spaces, and underline characters are allowed.</p>

## Interface Group Form: Additional Filters Tab

Additional Filters enable the NNMi administrator to use expressions to further define which interfaces to include in an Interface Group.

If any Additional Filters are created:

- NNMi first evaluates any ifType filters. Interfaces must match *all* specifications to belong to this Interface Group.
- NNMi then evaluates any Additional Filters expression. Interfaces *must also match all* Additional Filters expression specifications to belong to this Interface Group.



**Note:** The Additional Filters Editor requires that your user name be assigned a role of Administrator. If you are an NNMi Administrator, see the "Help for Administrators" for more information about how to use the Additional Filters Editor.

The ["Interface Group Form" \(on page 94\)](#) provides details about the selected Interface Group.

**For information about each tab:**

If an NNMi administrator created any Additional Filters for the selected Interface Group, NNMi displays the Additional Filters expression.

## Management Station Form

Management Station configurations are used for a variety of purposes:

- Enable NNM 6.x or 7.x to forward events to NNMi.
- Enable access to NNM 6.x or 7.x features from incidents that were forwarded from NNM 6.x/7.x. (See ["Accessing NNM 6.x and 7.x Features" \(on page 209\)](#) for more information.)
- Filter incident views by NNM 6.x or 7.x Management Station.

### NNM 6.x or 7.x Management Station Attributes

Name	Description
Name	The name your team uses to identify this remote NNM 6.x or 7.x management station.
NNM Version	The version of NNM (6.x or 7.x) in use on this remote management station.
IP Address	The IP address used for communication with this remote NNM 6.x or 7.x management station.
ovas Port (OpenView Application Server)	The port number used by the OpenView Application Server (ovas) on this NNM 6.x or 7.x management station.  The port number is usually 7510.
Web Server Port	The port number used by the web server on this NNM 6.x or 7.x management station: <ul style="list-style-type: none"> <li>• For NNM 7.x management stations on all operating systems, the port number is usually 3443.</li> <li>• For NNM 6.x management stations running UNIX, the port is usually 3443.</li> <li>• For NNM 6.x management stations running Windows systems, it is usually 80.</li> </ul>
Description	<i>Optional.</i> Notes your NNMi administrator added about this NNM 6.x or 7.x management station.  Maximum length 255 characters. Alpha-numeric, punctuation, spaces, and underline characters allowed.

## Viewing Maps (Network Connectivity)

NNMi provides several views that display maps of device connections within your network. You can access these views in the Troubleshooting workspace or by using the **Actions** → menu. These views include:

- [Layer 2 Neighbor View](#)
- [Layer 3 Neighbor View](#)
- [Path View](#)
- ["Node Group Maps" \(on page 99\)](#)

The OSI initiative identified seven layers for communication and computer network protocol design. The [Layer 2](#)<sup>1</sup> and [Layer 3](#)<sup>2</sup> Neighbor Views display data according to the Open Systems Interconnection (OSI) model.

The Path view combines real-time data about both Layer 2 and Layer 3 information.

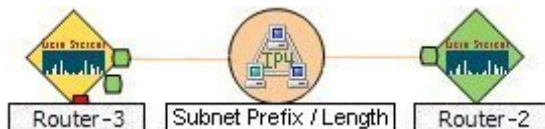
On the maps, the lines between devices indicate the connections.

In Layer 2 Neighbor View maps, interfaces that are connected to a neighbor are indicated by little squares around the background shape of the parent node. Pay special attention to the color of the lines, which represent connections. For example:



See [About Status Colors](#) for more information.

In Layer 3 Neighbor View maps, addresses connected to neighbors within the same IP subnet are indicated by little hexagons around the background shape of the parent node. The lines indicate the subnets, so the lines are beige (no status). For example:



Node Group Maps show the members of a Node Group (defined by the NNMi administrator). The map displays the status and connectivity of each member. Your NNMi administrator can also specify a background image (for example, a map of North America). Child Node Groups display the hierarchy of nodes in a Node Group.

---

<sup>1</sup>Refers to the Data Link layer of the multilayered communication model, Open Systems Interconnection (OSI). The Data Link layer moves data across the physical links in the network. The switches and bridges are devices that redirect data messages at the layer 2 level, using the destination Media Access Control (MAC) address to determine where to direct the message.

<sup>2</sup>Refers to the Network layer of the multilayered communication model, Open Systems Interconnection (OSI). The Network layer is concerned with knowing the address of the neighboring nodes in the network, selecting routes and quality of service, and recognizing and forwarding incoming messages to local host domains. The router and switch-router are the devices that redirect data messages at the Layer 3 level. Everything in a subnet is connected at the Layer 3 (IP) level.

## Node Group Maps

Node Group Maps enable you to see the members of a Node Group (defined by the NNMi administrator). The map displays the status and connectivity of each member. Your NNMi administrator can specify a background image (for example, a map of North America).

**Note:** If your role allows, you can configure the settings for a Node Group map, including selecting the background image. To do so, use the **File** → **Open Node Group Map Settings** option. See "Help for Administrators" for more information.

Because node membership is based on the Node Group, not connectivity, one or more nodes might not be connected on a Node Group Map.

### To display a Node Group Map using the Troubleshooting workspace:

1. From the **Workspaces** navigation panel, select the **Troubleshooting** workspace.
2. Select **Node Group Map**.
3. In the **Node Group** field, enter the name of the Node Group whose map you want to display.

**Note:** As you start typing the first few letters (case-sensitive) of the name of the node group you want to use, you will view a list that includes all potential node groups with names that match the letters as you enter them.

### To display a Node Group Map using the Actions menu:


1. From the **Workspaces** navigation panel, select the **Incident**, **Monitoring** or **Inventory** workspace.
2. From the **Incident** or **Monitoring** workspace, select **Node Groups**.
3. From the **Incident Management** or **Incident Browsing** workspace, select the Island Node Group incident view of interest.

**Note:** Incidents whose Source Object is an Island Node Group include **Remote site** in the incident message. See ["Island Node Group Map" \(on page 158\)](#) for more information.

4. In the Node Group or Incident view, click the  selection box that precedes the Node Group or Island Node Group incident of interest.
5. Select **Actions** → **Node Group Map**.



**Note:** When you use the Actions menu to display a map, each unique map appears in a new window. See [Using Actions to Perform Tasks](#) for more information.


When viewing nodes on a Node Group Map, keep in mind the following:

- By default, each Child Node Group is represented by a single hexagon that appears with the other Node objects of the Parent Node Group in the Node Group Map. Child Node Group objects can be moved and have their locations saved with other Node objects in the map. Unlike other Node objects, double-clicking a Child Node Group object displays a map of the nodes in the Child Node Group rather than the object's form.
- To display the nodes within a Child Node Group, do one of the following:
  - Double-click the Child Node Group object.
  - Select the Child Node Group object and do one of the following:
    - Click the  **Open Node Group Map** icon.
    - Select **Actions** → **(Child Node Group Name) Map**.

- An NNMi administrator alternatively can configure the map to display all nodes in a Child Node Group as though its contents are directly in the Parent Node Group by setting the **Expand Child in Parent Node Group Map** attribute. An NNMi administrator must set this option for each Child Node Group that should be expanded. See ["Node Group Hierarchy \(Child Node Group\) Form" \(on page 92\)](#) for more information.
- To view more information about the selected Node Group, open the Node Group form using the **File** → **Open Node Group for Map** option.
- NNMi enlarges any node on a Node Group map that has an open root cause incident associated with it. To view an associated incident for a node on a Node Group map, double-click the node of interest. In the Node form, select the Incidents tab.

To disable the open root cause indicator, clear the **Indicate Root Cause Incidents** check box in the map view toolbar.

To refresh node and Node Group status at any time, use the  **Refresh Status** icon. See [Refresh Only Node Status on a Map](#) for more information. You can also refresh connectivity, map objects, as well as node and Node Group status using the  **Refresh All** icon.

To return to the previous Node Group map, click the  **Back to Previous Node Group** icon. See ["Navigating within a Node Group Map" \(on page 100\)](#) for more information about ways to navigate within a Node Group Map. ["Navigating within a Node Group Map" \(on page 100\)](#)

NNMi provides the following Node Group Map views:

- ["Node Group Overview Map" \(on page 101\)](#)
- ["Network Overview Map" \(on page 102\)](#)
- ["Important Nodes Map"](#)
- ["Networking Infrastructure Devices Map" \(on page 102\)](#)
- ["Routers Map" \(on page 103\)](#)
- ["Switches Map" \(on page 103\)](#)



### Related Topics

["Navigating within a Node Group Map" \(on page 100\)](#)


["Position Nodes on a Node Group Map" \(on page 101\)](#)

## Navigating within a Node Group Map

Navigation and accessing node details on a Node Group Map are the similar to those for the Layer 2 Neighbor and Layer 3 Neighbor maps with the following exceptions:

- To display a Node Group map of a Child Node Group in the same window:
  - a. Double-click the Child Node Group object:  

  - b. Select the Child Node Group object and click the  **Open Node Group Map** icon.
- To display a Node Group Map for a Child Node Group in a new window, use **Actions** → **Node Group Map**.



**Note:** The Child Node Group map must be unique to be displayed in a new window. See [Using Actions to Perform Tasks](#) for more information.

- To return to the previous Node Group Map, use the  **Back to Previous Node Group** icon .

- To open the Node Group form for a Node Group map, select **File** → **Open Node Group for Map**.
- To open the Node Group Map Settings form from a Node Group map, select **File** → **Open Node Group Map Settings**.
- You can manually reposition the nodes on the background image, and, if your role allows, save the map for later use. See "[Position Nodes on a Node Group Map](#)" (on page 101) for more information.
- If **Indicate Key Incidents** is enabled, NNMi enlarges any node on a Node Group map that has an open Key Incident associated with it. To view an associated incident for a node on a Node Group map, double-click the node of interest. In the Node form, select the Incidents tab.

To enable the Key Incident indicator, select the **Indicate Key Incidents** check box in the map view toolbar.

To disable the Key Incident indicator, clear the **Indicate Key Incidents** check box in the map view toolbar.


As in other maps, clicking the  Open icon after selecting a node on the map, displays the Node form. Clicking the  Open icon after selecting a Child Node Group, opens the Child Node Group form. See [Use Map Views](#) and [Access More Details \(Quick View and Forms\)](#) for more information.


## Position Nodes on a Node Group Map

You can manually reposition the nodes on the map, and, if your role allows, save the map. NNMi users see your change the next time the map is refreshed.

**Note:** If your role allows, to return to the original layout that NNMi automatically determines, use **File** → **Clear Layout**.

**To position and save node locations on a Node Group Map view:**

1. Navigate to the Node Group Map:
  - a. From the workspace navigation panel, select the **Inventory** or **Monitoring** workspace.
  - b. Select **Node Groups**.
  - c. In the Node Group view, click the  selection box that precedes the Node Group of interest.
  - d. Select **Actions** → **Node Group Map**.
2. Manually re-position the node locations by dragging and dropping the nodes to the location you want.
3. If your role allows, select  **Save Layout** from the toolbar menu to save all node locations on the map.

**Note:** Each time you select  **Save Layout**, NNMi deletes any previous node location information for the map.

## Node Group Overview Map

This Node Group map displays all top-level Node Groups that have been configured for your network.

Use this view when you want to do any of the following tasks:

- Determine the Node Groups created for your network.
- Determine the Node Group hierarchy for the Node Groups created for your network.

**To display the Node Group Overview map using the Topology Maps workspace:**

1. From the workspace navigation panel, select the **Topology Maps** workspace.
2. Select **Node Group Overview**.

#### **Related Topics**

[Views Provided by NNMi](#)

[Node Group Map Objects](#)

## **Network Overview Map**

Displays a map containing the most highly connected nodes in the Layer 3 network. This map periodically updates both topology and status. The update interval is more frequent when the topology is changing, and less frequent when the topology is not changing.

**Note:** Automatic refresh cancels any modifications, such as selecting or zooming, you make to this view.

Use this view when you want to do any of the following tasks:

- View a high level overview of your network
- Determine the most highly connected nodes in the Layer 3 network
- Determine discovery progress

**To display the Network Overview map using the Topology Maps workspace:**

1. From the workspace navigation panel, select the **Topology Maps** workspace.
2. Select **Network Overview**.

#### **Related Topics**

[Views Provided by NNMi](#)

[Node Group Map Objects](#)

## **Networking Infrastructure Devices Map**

**Tip:** Your NNMi administrator can add or delete maps from the Topology Maps workspace. If the Networking Infrastructure Devices map is not available, your NNMi administrator might have chosen to remove this map from the Topology Maps workspace.

The Networking Infrastructure Device map provides representative Node Groups for the Switches and for the Routers in your network. Each of the following device types, if applicable, are also included on the map:

- Chassis
- Firewalls
- Voice Gateways

To view the connectivity within each device type (Node Group), click the Node Group of interest. See ["Node Groups View \(Inventory\)" \(on page 25\)](#) for more information about Node Groups.

Use this view when you want to do any of the following tasks:

- Determine the types of devices in your network.
- View the connectivity within a group of devices of the same type.
- Determine the number of devices of a specific type.

**To display the Networking Infrastructure Devices map using the Topology Maps workspace:**

1. From the workspace navigation panel, select the **Topology Maps** workspace.
2. Select **Networking Infrastructure Devices**.

### Related Topics

[Views Provided by NNMi](#)

[Node Group Map Objects](#)

## Routers Map

**Tip:** Your NNMi administrator can add or delete maps from the Topology Maps workspace. If the Routers Map is not available, your NNMi administrator might have chosen to remove this map from the Topology Maps workspace.

The Routers map shows a graphical representation of the Layer 3 connectivity in your network. Connector devices on Layer 3 maps are routers, switch-routers, and gateways. (See [About Map Symbols](#) for more information.)

**Note:** If the number of nodes in your network is greater than the maximum number of nodes configured to be displayed on the map, NNMi filters the map to display routers that have interfaces with addresses in the largest number of overall subnets in the network. This means that routers with little or no connectivity are only displayed for smaller networks.

Use this view when you want to do any of the following tasks:

- Understand the router connectivity between your devices.
- Determine the routers that are connected to the largest number of subnets.

**To display the Routers map using the Topology Maps workspace:**

1. From the workspace navigation panel, select the **Topology Maps** workspace.
2. Select **Routers**.

### Related Topics

[Views Provided by NNMi](#)

[Node Group Map Objects](#)

## Switches Map

**Tip:** Your NNMi administrator can add or delete maps from the Topology Maps workspace. If the Switches map is not available, your NNMi administrator might have chosen to remove this map from the Topology Maps workspace.

The Switches map shows a graphical representation of the Layer 2 connectivity in your network. Connector devices on Layer 2 maps are switches, ATM switches, and switch-routers. (See [About Map Symbols](#) for more information.)

**Note:** If the number of nodes in your network is greater than the maximum number of nodes configured to be displayed on the map, NNMi filters the map to display switches that are the most highly connected.

Use this view when you want to do any of the following tasks:

- Understand the switch connectivity between your devices.
- Determine the switches that are connected to the largest number of devices.

**To display the Switches map using the Topology Maps workspace:**

1. From the workspace navigation panel, select the **Topology Maps** workspace.
2. Select **Switches**.

### Related Topics

[Views Provided by NNMi](#)

[Node Group Map Objects](#)

## Display the Layer 2 Neighbor View

The [Layer 2](#)<sup>1</sup> Neighbor View shows a graphical representation of the selected device and any connections with other devices within a specified number of hops from the selected device. Connector devices on Layer 2 are switches and bridges. (See [About Map Symbols](#) for more information.)

Use this neighbor view when you want to do any of the following tasks:

- Understand the switch connectivity between your devices.
- Find the cause of a connectivity problem (the device status is not Normal).
- Identify the highly-connected nodes in your environment.
- Determine what else might be affected by a problem device, such as an interface.

**To display the Layer 2 Neighbor View using the Troubleshooting workspace:**

1. From the workspace navigation panel, select the **Troubleshooting** workspace.
2. Select **Layer 2 Neighbor View**.
3. In the **Node or IP** field, type the name or IP address of a node in your network. (NNMi provides a case-sensitive drop-down list to help speed up your selection.)
4. A hop is a node representing any network device, such as a workstation, gateway, or switch, which is connected by a link with no intermediate nodes.

Click the **Number of Hops** drop-down list, and select the number of hops to display (1-9). The default number of hops is 1.

5. All devices connected to the initial object within the specified number of hops are displayed.

---

<sup>1</sup>Refers to the Data Link layer of the multilayered communication model, Open Systems Interconnection (OSI). The Data Link layer moves data across the physical links in the network. The switches and bridges are devices that redirect data messages at the layer 2 level, using the destination Media Access Control (MAC) address to determine where to direct the message.



The color of the line between the devices indicates the health of the connection ( See ["Viewing Maps \(Network Connectivity\)" \(on page 98\)](#)).

A mesh connection represents the location of multiple devices interconnected with each other. A mesh is represented by the following icon:



**To display the Layer 2 Neighbor View using the Actions menu in a table view or in a form:**

1. From the workspace navigation panel, select the table view of interest.

For example the **Inventory** → **Nodes** view.

2. Select the object instance of interest (node, interface, or address).

For example, click the  selection box that precedes the node of interest from the **Nodes** view.

3. Select **Actions** → **Layer 2 Neighbor View**. The starting node appears with a bold label on a map.

**Note:** When you use the **Actions** menu to display a map, each unique map appears in a new window. See [Using Actions to Perform Tasks](#) for more information.

4. A hop is node representing any network device, such as a workstation, gateway, or switch, which is connected by a link with no intermediate nodes.

Click the **Number of Hops** drop-down list, and select the number of hops to display (1-9). The default number of hops is 1.



5. All devices connected to the initial object within the specified number of hops are displayed.

The color of the line between the devices indicates the health of the connection ( See ["Viewing Maps \(Network Connectivity\)" \(on page 98\)](#)).

A mesh connection represents the location of multiple devices interconnected with each other. A mesh is represented by the following icon:



**To see more information about a specific connection on the map:**

1. Select the line or  (mesh connection) icon of interest.
2. Click the  Open icon on the map toolbar.
3. The Layer 2 Connection form displays, showing all information for the connection. See ["Layer 2 Connection Form" \(on page 106\)](#) for information.

**To view the addresses for a particular interface:**

1. Click to select the interface of interest.

**Note:** If the interface is difficult to select, use the + (plus) key to zoom in on the map.

2. From the map view toolbar, select the  Open icon.

3. In the **Interface** form, select the **Addresses** tab.
4. Each address associated with the interface appears in the IP addresses table.

**To view the port number for an interface:**

Click the interface of interest.

The port number for the interface appears as a new label.

**To view the interface name at each end of a connection:**

Click the line representing the connection.

The interface name for each end of the connection appears as a new label.

**Tip:** Use Ctrl-Click to select multiple lines and display more interface names.

**Related Topics:**

[Using Map Views](#)








["Layer 2 Connection Form" \(on page 106\)](#)


## Layer 2 Connection Form

The Layer 2 Connection form provides details about a managed connection. These details include the interfaces that make up the connection, the protocol used to create this connection, and the current status of the connection. For example, if all interfaces are down within a connection, the connection status is listed as Critical.

**For information about each tab:**

**Basic Attributes**

Attribute	Description
Name	Name that NNMi assigned to the Layer 2 Connection. This name contains the list of member interface names separated by a comma. Each interface name appears in the format: <i>Node_Name[Interface_Name]</i> .
Status	Overall status for the current connection. NNMi follows the ISO standard for status classification. See the <a href="#">"Layer 2 Connection Form: Status Tab" (on page 108)</a> for more information. Possible values are:   No Status  Normal  Disabled  Unknown  Warning  Minor  Major


Attribute	Description
	<p> Critical</p> <p>For information about how the current status was determined, see the "<a href="#">Layer 2 Connection Form: Conclusions Tab</a>" (on page 109). Status reflects the most serious outstanding conclusion. See "<a href="#">Watch Status Colors</a>" (on page 129) for more information about possible status values.</p> <p><b>Note:</b> The icons are displayed only in table views.</p>
Topology Source	<p>Indicates the data source used to create this connection:</p> <p><b>CDP</b> - Cisco Discovery Protocol</p> <p><b>EDP</b> - Extreme Discovery Protocol</p> <p><b>ENDP</b> - Enterasys Discovery Protocol (also known as CDP - Cabletron Discovery Protocol)</p> <p><b>FDB</b> - Forwarding Database (also known as AFT - Address Forwarding Table on a bridge/switch)</p> <p><b>FDP</b> - Foundry Discovery Protocol</p> <p><b>LLDP</b> - Link Layer Discovery Protocol</p> <p><b>MLT</b> - Multi-Link Trunk technology (<i>NNMi Advanced</i>)</p> <p><b>PAgP</b> - Cisco Systems Port Aggregation Protocol (<i>NNMi Advanced</i>)</p> <p><b>SONMP</b> - SynOptics Network Management Protocol</p> <p><b>SUBNET CONNECTION</b> - Subnet Connection Rule. See "Help for Administrators" for more information.</p> <p><b>USER</b> - This connection was configured by your NNMi administrator (using the Connection Editor). See "Help for Administrators" for more information.</p>
Notes	<p>Provided for network operators to use for any additional notes required to further explain the Layer 2 connection. Information might include when a cable was last replaced.</p> <p>Type a maximum of 1024 characters. Alpha-numeric, punctuation, spaces, and underline characters are allowed.</p>

## Layer 2 Connection Form: Interfaces Tab

The "[Layer 2 Connection Form](#)" (on page 106) provides details about a managed connection. These details include the interfaces that make up the connection, the protocol used to create this connection, and the current status of the connection. For example, if all interfaces are down within a connection, the connection status is listed as Critical.

For information about each tab:

### Interfaces Table

Attribute	Description
Interfaces	<p>Table view of both of the interfaces that are part of the current connection. You can use this table to determine the status, administrative state, operational state, name, type, interface speed, and Layer 2 connection for each interface associated with the selected Layer 2 Connection.</p> <p>Click the  Open icon to view more information about a specific interface.</p>


Attribute	Description
-----------	-------------

## Layer 2 Connection Form: Incidents Tab

The "[Layer 2 Connection Form](#)" (on page 106) provides details about a managed connection.

For information about each tab:

### Incidents Table









Attribute	Description
Associated Incidents	<p>Table view of the incidents associated with the selected Layer 2 connection. These incidents are sorted by creation time so that you can view the incidents in chronological order. Use this view to determine which incidents are still open for the selected connection.</p> <p>Click the  Open icon to open the "<a href="#">Incident Form</a>" (on page 134) and view more information about a specific incident.</p>


## Layer 2 Connection Form: Status Tab

The "[Layer 2 Connection Form](#)" (on page 106) provides details about a managed connection.

For information about each tab:

### Status Attributes

Attribute	Description
Status	<p>Overall status for the current connection. NNMi follows the ISO standard for status classification. Possible values are:</p> <ul style="list-style-type: none"><li> No Status</li><li> Normal</li><li> Disabled</li><li> Unknown</li><li> Warning</li><li> Minor</li><li> Major</li><li> Critical</li></ul> <p>For information about how the current status was determined, see "<a href="#">Layer 2 Connection Form: Conclusions Tab</a>" (on page 109). Status reflects the most serious outstanding conclusion. See "<a href="#">Watch Status Colors</a>" (on page 129) for more information about possible status values.</p> <p><i>NNMi Advanced.</i> If the Layer 2 Connection is an Aggregator Link, the Status is calculated using the Status of the Aggregator Interface members. Click here for more information.</p> <p>An Aggregator Link Status of <b>Minor</b> indicates the Status of at least one of the Aggregator Interfaces that is a member of the Aggregator Link is <b>Minor</b>. A Status of <b>Critical</b> indicates the Status of at least one of the Aggregator Interfaces that is a member of the Aggregator Link is</p>


Attribute	Description
	<p><b>Critical.</b></p> <p>Also see <a href="#">Layer 2 Neighbor View Map Objects</a>.</p> <p><b>Note:</b> The icons are displayed only in table views.</p>
Status Last Modified	Date and time indicating when the status was last set.
Status History	<p>List of up to the last 30 changes in status for the selected connection. This view is useful for obtaining a summary of the connection status so that you can better determine any patterns in connection behavior and activity.</p> <p>Click the  Open icon to view more information about a specific status.</p>

## Layer 2 Connection Form: Conclusions Tab

The "[Layer 2 Connection Form](#)" (on page 106) provides details about a managed connection.

For information about each tab:

### Conclusions Table (for Status)

Attribute	Description
Status Conclusions	<p>The dynamically generated list of summary statuses of the connection at points in time that contributed to the current overall status of the selected connection. Status is set by Causal Engine.</p> <p>Each conclusion listed is still outstanding and applies to the current overall status.</p> <p>This view is useful for obtaining a quick summary of the status and problem description for the current connection that led up to the connection's most current status.</p> <p>Examples of conclusions that might appear together are listed below:</p> <ul style="list-style-type: none"> <li>• SNMP Agent Not Responding</li> <li>• Interface Down</li> <li>• Address Down</li> </ul> <p>The status value is correlated based on the most critical conclusions. Click the  Open icon to view more information about a specific conclusion.</p>

## Layer 2 Connection Form: Link Aggregation Tab (NNMi Advanced)



The "[Layer 2 Connection Form](#)" (on page 106) provides details about the selected Layer 2 connection.

For information about each tab:

The Layer 2 Connection Form: Link Aggregation Tab provides information about the **Link Aggregation**<sup>1</sup> in which the Layer 2 Connection belongs. This tab only appears if the selected Layer 2 Connection participates in a Link Aggregation protocol. The contents of the tab differ based on the Layer 2 Connection's role in the Link Aggregation (Member or Aggregator).

A Member Layer 2 Connection's Link Aggregation Tab displays the Link Aggregation protocol and a reference to the Aggregation's Aggregator Layer 2 Connection. Click here for more details about the attributes displayed.

### Link Aggregation Tab


Attribute	Description
Link Aggregation Protocol	<p>Protocol used to create the Link Aggregation, including the Aggregator Layer 2 Connection and its physical Members. Possible values include:</p> <ul style="list-style-type: none"> <li>• Cisco Systems Port Aggregation Protocol (pagp)</li> <li>• Multi-Link Trunk technology (mlt)</li> <li>• Split Mutli-Link Trunk technology (splitMlt)</li> <li>• Inter-switch trunk that is part of a Split Multi-Link Trunk configuration (istMlt)</li> </ul> <p><b>Note:</b> In rare cases, it is possible for a Layer 2 Connection to connect sets of Aggregator/Member Interfaces that are configured using different Link Aggregation protocols. In these cases, the Layer 2 Connection's Link Aggregation Protocol attribute value contains multiple protocols separated with a slash (/).</p>
Aggregator	<p>Name of the Aggregator Layer 2 Connection that is part of the Link Aggregation. The Aggregator represents the collection of physical Layer 2 Connections that are Members of the Link Aggregation.</p> <p>See <a href="#">Layer 2 Neighbor View Map Objects</a> for more information.</p> <p>The name value is the Name that the NNMi administrator provided to identify this Layer 2 Connection.</p> <p>Click the  Lookup icon, and choose  Open to open the form for the Aggregator Link.</p>

The Aggregator Layer 2 Connection's Link Aggregation Tab lists the Member Layer 2 Connections of the Link Aggregation and provides cumulative bandwidth statistics for the Link Aggregation Layer 2 Connections. Click here for more details of the attributes displayed.

---

<sup>1</sup>A Link Aggregation is comprised of an Aggregator Link, Aggregator Interface, and the physical interfaces and connections that they represent. An Aggregator Link object represents many-to-many physical connections. For example, two nodes might be connected with four physical connections. These four physical connections are depicted as a single Aggregator Link object using a thick line on the Layer 2 Neighbor View map. The interface depicted at each end of the Aggregator Link object is an Aggregator Interface object. An Aggregator Interface object represents the collection of physical interfaces for one end of an Aggregator Link.

### Link Aggregation Tab

Attribute	Description
Link Aggregation Protocol	<p>Protocol used to create the Link Aggregation, including the Aggregator Interface and its physical Members. Possible values include:</p> <ul style="list-style-type: none"> <li>• Cisco Systems Port Aggregation Protocol (pagp)</li> <li>• Multi-Link Trunk technology (mlt)</li> <li>• Split Mutli-Link Trunk technology (splitMlt)</li> <li>• Inter-switch trunk that is part of a Split Multi-Link Trunk configuration (istMlt)</li> </ul> <p><b>Note:</b> In rare cases, it is possible for a Layer 2 Connection to connect sets of Aggregator/Member Interfaces that are configured using different Link Aggregation protocols. In these cases, the Layer 2 Connection's Link Aggregation Protocol attribute value contains multiple protocols separated with a slash (/).</p>
Available Bandwidth	The lowest Available Bandwidth value of the Aggregator Interfaces connected by this Layer 2 Connection.
Maximum Bandwidth	The lowest Maximum Bandwidth value of the Aggregator Interfaces connected by this Layer 2 Connection.
Available Bandwidth Percentage	Percentage value computed using the Available Bandwidth divided by the Maximum Bandwidth values.
Members	<p>Table view of the Layer 2 Connections that are Members of the selected Aggregator Link.</p> <p>Click the  Open icon to view more information about a specific Layer 2 Connection.</p>

### Layer 2 Connection Form: Registration Tab

The "[Layer 2 Connection Form](#)" (on page 106) provides details about a managed connection.

For information about each tab:

#### Registration

Attribute	Description
Created	Date and time the selected object instance was created. NNM uses the locale of the client and the date and time from the NNMi management server.
Last Modified	Date the selected object instance was last modified. NNM uses the locale of the client and the date and time from the NNMi management server.

## Display the Layer 3 Neighbor View

The [Layer 3](#)<sup>1</sup> Neighbor View is a graphical representation of the subnets in which the starting node participates, and the health of the routers in those subnets. Connector devices on Layer 3 are routers and switch/routers. (See [About Map Symbols](#) for more information.)

Use this neighbor view when you want to do any of the following tasks:

- Determine whether a subnet is down.
- Understand the router connectivity between your devices.
- Assist in finding the root cause of a connectivity problem (see which device along the communication chain has a status other than normal).
- Identify the highly-connected nodes in your environment.

### To display a Layer 3 Neighbor View using the Troubleshooting workspace:

1. From the workspace navigation panel, select the **Troubleshooting** workspace.
2. Select **Layer 3 Neighbor View**.
3. In the **Node or IP** field, type the name or IP address of a node in your network. (NNMi provides a case-sensitive drop-down list to help speed up your selection.)
4. A hop represents any network device, such as a workstation, gateway, or switch, that is connected by a link with no intermediate nodes.

Click the **Number of Hops** drop-down list, and select the number of hops to display (1-9). The default number of hops is 1.

5. All devices connected to the initial object within the specified number of hops are displayed.

The color of the line between the devices indicates the health of the subnet between the devices (see ["Viewing Maps \(Network Connectivity\)" \(on page 98\)](#)).

### To display the Layer 3 Neighbor View using the Actions menu in a table view or in a form:

1. From the workspace navigation panel, select the table view of interest.  
For example the **Inventory** → **Nodes** view.
2. Select the initial object of interest.  
For example, click the  selection box that precedes the node of interest from the **Nodes** view.
3. Select **Actions** → **Layer 3 Neighbor View**.  
**Note:** When you use the **Actions** menu to display a map, each unique map appears in a new window. See [Using Actions to Perform Tasks](#) for more information.
4. A hop represents any network device, such as a workstation, gateway, or switch, that is connected by

---

<sup>1</sup>Refers to the Network layer of the multilayered communication model, Open Systems Interconnection (OSI). The Network layer is concerned with knowing the address of the neighboring nodes in the network, selecting routes and quality of service, and recognizing and forwarding incoming messages to local host domains. The router and switch-router are the devices that redirect data messages at the Layer 3 level. Everything in a subnet is connected at the Layer 3 (IP) level.




a link with no intermediate nodes.

Click the **Number of Hops** drop-down list, and select the number of hops to display (1-9). The default number of hops is 1.

5. All devices connected to the initial object within the specified number of hops are displayed.

The color of the line between the devices indicates the health of the connection (see "[Viewing Maps \(Network Connectivity\)](#)" (on page 98)).

**To see more information about a specific subnet on the map:**

1. Select the line that represents the subnet of interest.
2. Click the  Open icon on the map toolbar.

The IP Subnet form displays, showing all details of the subnet. See "[IP Subnet Form](#)" (on page 113) for more information.

**To view address information for an interface at each end of a connection:**

Click the line representing the connection of interest.

The IP address for each interface appears as a new label.

**Tip:** Use Ctrl-Click to select multiple lines and display more IP addresses.

**Related Topics:**

[Using Map Views](#)

## IP Subnet Form

The IP Subnet form provides details about the selected subnet.

If your role allows, you can add notes to communicate information about this subnet to your team.

**For information about each tab:**

**Basic Attributes**

Attribute	Description
Name	Subnet for the IP network. This value is determined by the discovery process (calculated from IP Addresses and the subnet prefix information).
Prefix	The value of the prefix for the current subnet (also known as the subnet address).
Prefix Length	The number of significant bits in the subnet prefix. This value is used to determine the size of the subnet.
Notes	Provided for network operators to use for any additional notes required to further explain the subnet. Information might include its use; for example, point to point for dialup. You might also use this attribute to track which geographical group might use the subnet.  Type a maximum of 1024 characters. Alpha-numeric, punctuation, spaces, and underline characters are allowed.

Attribute	Description
-----------	-------------

**Note:** You can sort your subnet table views based on this value. Therefore, you might want to include keywords for this attribute value.

## IP Subnet Form: IP Addresses Tab


The "IP Subnet Form" (on page 113) provides details about the selected subnet.

For information about each tab:

### IP Addresses Table

Attribute	Description
-----------	-------------

IP Addresses Table view of the IP addresses associated with the selected subnet. You can use this table to determine the state, address, and interface, and parent node for each address associated with the selected subnet.

Click the  Open icon to open the "IP Address Form" (on page 73) and view more information about a specific address.

## IP Subnet Form: Registration Tab

The "IP Subnet Form" (on page 113) provides details about the subnet selected.

For information about each tab:

### Registration

Attribute	Description
-----------	-------------

Created Date and time the selected object instance was created. NNM uses the locale of the client and the date and time from the NNMi management server.

Last Modified Date the selected object instance was last modified. NNM uses the locale of the client and the date and time from the NNMi management server.

## Path Between Two Nodes that Have IPv4 Addresses

**Note:** If NNMi Advanced is licensed and installed, also see "Enhanced Path View (NNMi Advanced)" (on page 118).

Path View calculates the route that data flows between two nodes, and provides a map of that information. The two nodes can be any combination of end nodes, switches, or routers.

**Note:** End nodes are the primary use case for this view. If you specify switches or routers as the Source or Destination, the path is a best effort.

Each connection between the two nodes is a line on the map. If more than one route is possible, NNMi uses a set of rules to choose the displayed route (see "Path Calculation Rules" (on page 116)). NNMi indicates there is more than one possible path under either of the following conditions:

- *NNMi Advanced.* NNMi finds more than one Active router in a Router Redundancy Group. See "Router Redundancy Group View (NNMi Advanced)" (on page 24) for more information about Router

Redundancy Groups. See ["Path Calculation Rules" \(on page 116\)](#) for more information about Active router paths.


- *NNMi Advanced.* HP Router Analytics Management System (RAMS) determines more than one equal cost path and, therefore, cannot determine which path is in use. See ["Enhanced Path View \(NNMi Advanced\)" \(on page 118\)](#) for more information.



**Note:** Your NNMi administrator can configure Path View connections using a `PathConnections.xml` file. This file enables Path View to traverse undiscovered regions of your network. Each time NNMi determines a node in the Path View, NNMi checks whether the node is specified as a Start node in the `PathConnections.xml` file. If the node is specified as a Start node, each path segment configured in `PathConnections.xml` is inserted in the Path View map.

*NNMi Advanced.* When RAMS data is used to determine the router paths, NNMi ignores the `PathConnections.xml` file. See ["Enhanced Path View \(NNMi Advanced\)" \(on page 118\)](#) for more information.


Path View is a *flow diagram* rather than a *connection diagram*. It displays the flow of network traffic rather than all of the available connections. To view all possible connections between nodes, use the Layer 2 Neighbor View. See ["Display the Layer 2 Neighbor View" \(on page 104\)](#) for more information.

**Note:** Intermediate devices that are physically connected might appear in a Path View. For example, if two end nodes connect to the same switch, but exist in different VLANs, the path includes the access router where the VLAN and subnet determination is made.

Path View is useful for diagnosing connectivity problems. Path View shows each switch (and the port on that switch) that participates in the current path. You can quickly identify problematic switch ports that need to be shut down. Select any map symbol and click the  Open icon to display all known details about that object. Mouse over any object on the map to access the Quick View information about that object.

**Tip:** Click the  Swap icon to switch the **Source** and **Destination** values, and then click the  Compute Path. Sometimes NNMi can detect more information from one direction or the other.

#### Using Path View from the Troubleshooting workspace:


1. From the workspace navigation panel, select the **Troubleshooting** workspace.
2. Select **Path View**.
3. In the **Source** field, type the name or IPv4 address of a node in your network. (NNMi provides a case-sensitive drop-down list to help speed up your selection.)
4. *Optional.* In the **Destination** field, type a node name or IPv4 address.  
If a **Destination** value is not provided, NNMi displays the path from the **Source** node to its access router.
5. Click the  Compute Path icon.

#### Using Path View from the Actions menu in a table view or in a form:

1. Access a table view of nodes, interfaces, or IPv4 addresses.
2. Decide which object you want to use as the starting point in the path (**Source**). Click the  selection box in the row representing that object.
3. *Optional.* Decide which object you want to use as the destination point in the path (**Destination**). Click the  selection box in the row representing that object.  
If a **Destination** value is not provided, NNMi displays the path from the **Source** node to its access router.

4. In the menu bar, select **Actions** → **Path View**.

**Note:** When you use the **Actions** menu to display a map, each unique map appears in a new window. See [Using Actions to Perform Tasks](#) for more information.

5. Click the  Compute Path icon to display the map of the path.

**Related Topics:**

["Path Calculation Rules" \(on page 116\)](#)

["Investigate Errors and Performance Issues" \(on page 118\)](#)

["Access Node Details" \(on page 130\)](#)

## Path Calculation Rules

**Note:** If NNMi Advanced is licensed and installed, also see ["Enhanced Path View \(NNMi Advanced\)" \(on page 118\)](#)

Path View calculates the active flow of data between devices at the time the view is requested. The active path includes the following devices:


- Source and destination nodes
- Layer 2 devices between the source node and its access router
- Layer 2 devices between the destination node and its access router
- Layer 2 and Layer 3 routing core between the two access routers

**Note:** The path calculated can include one or more VLANs when applicable.

NNMi starts with the specified source and follows the active path to the specified destination. If no missing connections are detected, the Path View shows the source node, destination node, and each router and switch in between.

**Note:** Your NNMi administrator can configure Path View connections using a `PathConnections.xml` file. This file enables Path View to traverse undiscovered regions of your network. Each time NNMi determines a node in the Path View, NNMi checks whether the node is specified as a Start node in the `PathConnections.xml` file. If the nodes is specified as a Start node, each path segment configured in `PathConnections.xml` is inserted in the Path View map.

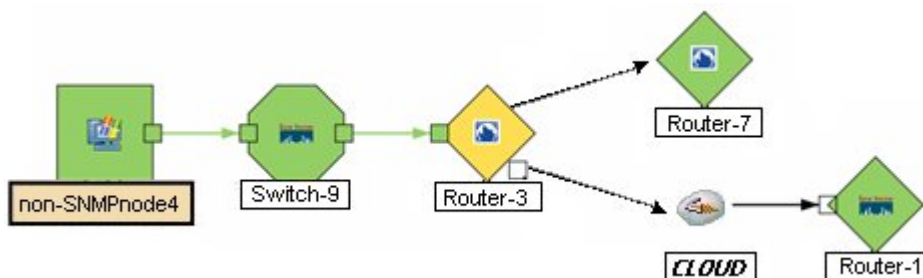
*NNMi Advanced.* When RAMS data is used to determine the router paths, NNMi ignores the `PathConnections.xml` file. NNMi also shows all Equal Cost Multi-Paths (ECMP). See ["Enhanced Path View \(NNMi Advanced\)" \(on page 118\)](#) for more information.

A  cloud symbol can represent the following types of information. The map can include multiple cloud symbols:

- If a missing connection is detected (no response to SNMP and no entry in `PathConnections.xml`), the cloud symbol appears in the routing core between the access routers.
- If the port connecting the end node to the first switch is forwarding more than one MAC address, this indicates an intermediate device (such as a hub or one or more undiscovered switches). A cloud appears at that location in the path.

When interpreting Path View results, note the following:

- The Source and Destination nodes must meet **either** of the following criteria:
  - Support SNMP and be previously discovered by NNMi (recorded in the topology database)
  - Have traceroute available
- All access routers and any Layer 2 devices between the Source and Destination nodes must meet the following criteria:
  - Support SNMP
  - Be previously discovered by NNMi (recorded in the topology database)
- *Optional*. Each router and switch is monitored by NNMi.
- The time stamp provided in the final Path View is the time at which the final active path was determined.
- *NNMi Advanced*. If the Router Redundancy Group has more than one Active router, NNMi selects one Active router for the path. To indicate there is more than one possible path, NNMi connects any additional Active routers to the chosen router as shown in the following example:



(*NNM iSPI Performance for Metrics*) You can access performance data from Path Views that contain single or multiple paths. See ["Investigate Errors and Performance Issues" \(on page 118\)](#) for more information.

#### Related Topics:

[Use Map Views](#) (and accessing Quick View information)

["Path View Limitations" \(on page 117\)](#)

### Path View Limitations

Path View cannot calculate accurate paths if you have two or more areas of your network which are separated by undiscovered devices. Your NNMi administrator must use the `PathConnections.xml` file to specify areas of your network that are separated by undiscovered devices. See "Help for Administrators" for more information.

Path View uses a variety of sources for information to calculate an accurate path. These sources of information do, however, have limitations:

- SNMP ipRoute tables. If the Source or Destination node represents a device other than a router and the device does not support SNMP or does not return valid ipRoute table information, NNMi depends on traceroute to follow the path to find the nodes's access router.

**Note:** *NNMi Advanced*. NNMi can use RAMS data to determine router paths. When RAMS data is used to determine the router paths, NNMi ignores the `PathConnections.xml` file. See ["Enhanced Path View \(NNMi Advanced\)" \(on page 118\)](#) for more information.

- Open Shortest Path First protocol or Cisco Global Load Balancing protocol. Path View shows the access router selected by one of these routing protocols. If two or more access routers communicate with a device, only one access router is shown (usually the one with the shortest path).
- Cisco Express Forwarding protocol. This protocol bypasses some of the data that Path View needs. If any routers in the path are using this protocol, Path View might display an incorrect router path.

## Investigate Errors and Performance Issues

The color of the background shape of each map symbol conveys the most recent health status. Select an object on the Path View map that has a status color other than green (see ["Watch Status Colors" \(on page 129\)](#) for more information about interpreting non-normal status colors). You can access the following types of information about each node:

- ["Access Node Details" \(on page 130\)](#)
- ["Access a Problem Device" \(on page 129\)](#)
- ["Access All Related Incidents" \(on page 130\)](#)

See ["Interpret Root Cause Incidents" \(on page 181\)](#) for more information about interpreting the incident information displayed.

(*NNM iSPI Performance for Metrics*) Click here for more information about additional tools for accessing performance data.

### To access performance data from a Path View map:

Select **Actions** → **Reporting - Path Health**.

If the Path View map contains multiple possible paths from the Source to Destination Node, NNMi alerts and guides you to select a single, unambiguous path for analysis before it can present a Path Health Report. You can bypass this interaction by pre-selecting enough map objects (for example, connections) to resolve any ambiguities before selecting **Actions** → **Reporting - Path Health**.

## Enhanced Path View (NNMi Advanced)

NNMi Advanced uses any of the following when calculating a Path View:

- Hot Standby Router Protocol (HSRP) nodes
- Virtual Router Redundancy Protocol (VRRP) nodes
- HP Router Analytics Management System (RAMS) data

**Note:** When using RAMS data in Path View, NNMi ignores the `PathConnections.xml` file. See "Help for Administrators" for more information.

When using NNMi Advanced, more than one path might appear if HP Router Analytics Management System (RAMS) determines more than one equal cost path and, therefore, cannot determine which path is in use. Also see [RAMS Data and Path View](#) below.

### HSRP and VRRP and Path View

If NNMi Advanced is licensed and installed, by default, NNMi monitors state and priority information for any discovered HSRP and VRRP objects in the network. NNMi Advanced can then include these virtual HSRP

and VRRP devices when calculating the Path View. The routers included are the Active or Master router in the HSRP or VRRP Group.

#### **RAMS Data and Path View**

If your NNMi Administrator configured one or more RAMS, NNMi Advanced calculates the Path View using RAMS data. (RAMS is an IP Route Analytics tool that listens to routing protocols and builds a real-time routing topology map.)

RAMS enhances NNMi's ability to trace the route path between the source and destination node in the following ways:

- NNMi Advanced does not use SNMP to calculate the router path. This means that NNMi Advanced does not need to wait for SNMP responses and can calculate the Path View more quickly.
- NNMi Advanced displays equal cost paths when calculating the router path.

## Monitoring Devices for Problems

NNMi offers several out-of-the-box views to assist you in monitoring your network. When using views, you can choose to do either of the following:

- Monitor views that contain your critical nodes and interfaces.
- Watch an incident view for incidents with an abnormal status, such as **Warning**, **Minor**, **Major**, or **Critical**.
- Watch a map view for any icons that change color to yellow or red.

No matter which way you prefer, you can navigate from a map to a table view or from a table view to a map.

### Related Topics:

["Filter Views by Node or Interface Group" \(on page 16\)](#)

["Monitor with Table Views" \(on page 120\)](#)

["Monitor with Map Views" \(on page 128\)](#)

## Monitor with Table Views

NNMi provides the following out-of-the-box node and interface views to assist you in monitoring the network for problems. These views help you quickly identify the nodes and interfaces that need your more immediate attention:

["Critical Interfaces View" \(on page 120\)](#)

["Critical Nodes View" \(on page 121\)](#)

["Non-Normal Interfaces View" \(on page 122\)](#)

["Non-Normal Nodes View" \(on page 122\)](#)

["Not Responding Address View" \(on page 124\)](#)

## Critical Interfaces View

**Tip:** See ["Interface Form" \(on page 60\)](#) for more details about the interface attributes that appear in this view's column headings.

The Critical Interfaces view is provided so that you can view all of your interfaces whose status is **Critical**.

For each interface displayed in the view, you can identify the interface's status, administrative (**AS**) and operational (**OS**) state, associated node Name value (**Hosted On Node**), the interface name, interface type, interface speed, its description, the interface alias, the date the interface status was last modified, the name of the Layer 2 connection associated with the interface, and any notes related to the interface.

By default, this view is sorted by the date the interface status was last modified (**Status Last Modified**).

See ["Interfaces View \(Inventory\)" \(on page 17\)](#) for more information about ways to use an interface view.

### Related Topics

[Use Table Views](#)



## Critical Nodes View

**Tip:** See ["Node Form" \(on page 28\)](#) for more details about the node attributes that appear in this view's column headings.

The Critical Nodes view in the Monitoring workspace is useful for identifying all of the nodes whose status is critical. Sorting the view by system location (the current value of the sysLocation MIB variable) might help you identify whether the problem can be isolated to a particular area of your network. You can also use this view to obtain the contact information for a problem node in case you need more background information to troubleshoot the problem.

For each node displayed, you can identify its status, device category, name, hostname, management address, system location, device profile, the date and time its status was last changed, and any notes included for the node.

The device profile information determines how devices of this type are managed and the icon and background shape displayed on maps.

By default, this view is sorted by the date the node status was last modified (**Status Last Modified**).

Node views are useful for quickly identifying items described in the following table.

### Uses for the Nodes Views

Use	Description
View all device types being managed	Sort the view by the <b>Device Profile</b> attribute.
Identify whether the problem can be isolated to a particular area of your network	Sort the view by <b>System Location</b> . This is the current value of the sysLocation MIB variable.
View address and subnet information associated with a selected node to better determine the scope of the problem	From the Nodes view, open the Node form. Then access the Address tab. See <a href="#">"Node Form" (on page 28)</a> and <a href="#">"IP Subnet Form" (on page 113)</a> for more information.
Access a map view of a selected node and its surrounding topology	Select the node of interest and use the Actions menu from the main toolbar. See <a href="#">"Viewing Maps (Network Connectivity)" (on page 98)</a> for more information.
View the statuses of interfaces associated with a node	If a node is not completely down, you might want to see which interfaces are down for the selected node. To do so, open the Node form and select the Interfaces tab. See <a href="#">"Interface Form" (on page 60)</a> for more information about interface attributes.
View the number of devices that are served by this node.	Select the node you want and access the Layer 2 or Layer 3 Neighbor View using the Actions menu.

## Critical Component View

**Tip:** See ["Node Form" \(on page 28\)](#) for more details about the attributes that appear in this view's column headings.

The Critical Component view in the Monitoring workspace is useful for identifying all of the nodes whose status is Critical due to a problem with a node component. Examples of node components include temperature, fan, and memory.

For each component displayed, you can see its status, name, type, and the node on which it resides.

## Non-Normal Interfaces View

**Tip:** See ["Interface Form" \(on page 60\)](#) for more details about the interface attributes that appear in this view's column headings.

The Non-Normal Interfaces view in the Monitoring workspace is useful for identifying all of the network interfaces that might need operator attention. Possible statuses for these interfaces include:

- Warning
- Major
- Minor
- Critical

**Note:** Interfaces displayed in this table all have the Administrative State equal to Up.

For each interface displayed in the view, you can identify its status, operational state, associated node Name value (**Hosted On Node**), the interface name, type, speed, a description of the interface, the ifAlias value, the date and time the status of the interface was last modified, the name of the Layer 2 connection associated with the interface, and any notes included for the interface.

By default, this view is sorted by the date the interface status was last modified (**Status Last Modified**).


Interface views are useful for quickly identifying items described in the following table.

Use	Description
View all network interfaces per node	Sort the view by <b>Hosted On</b> . This can help you organize your interfaces per node, so that you can identify the nodes that might need attention.
Determine the health of each of the managed interfaces	Sort the view by the <b>Status</b> attribute. To view only those interfaces whose status is <b>Critical</b> , use the <b>Critical Interfaces</b> view provided by NNMi. See <a href="#">"Critical Interfaces View" (on page 120)</a> for more information.
Determine the types of interfaces that are being managed.	Sort on the <b>IfType</b> (interface type) attribute.
Access a map view of the network interface and its surrounding topology.	Select the interface of interest and use the <b>Actions</b> menu to select either the Layer 2 or Layer 3 Neighbor View. See <a href="#">Use Table Views</a> for more information.

## Non-Normal Nodes View

**Tip:** See ["Node Form" \(on page 28\)](#) for more details about the node attributes that appear in this view's column headings.

The Non-Normal Nodes view in the Monitoring workspace is useful for identifying all of the nodes that might need your attention. Possible statuses for these nodes include:

 Warning

 Minor

 Major

 Critical

For each node displayed, you can identify its status, device category (for example, Switch), hostname, management address, system location (the current value of the sysLocation MIB variable), device profile, the date and time its status was last changed, and any notes included for the node.

The device profile information determines how devices of this type are managed and the icon and background shape displayed on maps.

By default, this view is sorted by the date the node status was last modified (**Status Last Modified**).

Node views are useful for quickly identifying items described in the following table.

Use	Description
View all problem nodes	Sort the view by Status so that you can be quickly alerted to existing and potential problems.  You can also access the Critical Nodes view provided by NNMi. See <a href="#">"Critical Nodes View" (on page 121)</a> for more information.
Identify whether the problem can be isolated to a particular area of your network	Sort the view by <b>System Location</b> . This is the current value of the sysLocation MIB variable.
View all device types being managed	Sort the view by the Device Profile attribute.
View address and subnet information associated with a selected node to better determine the scope of the problem	From the Nodes view, open the Node form. Then access the Address tab. See <a href="#">"Node Form" (on page 28)</a> and <a href="#">"IP Subnet Form" (on page 113)</a> for more information.
Access a map view of a selected node and its surrounding topology	Select the node of interest and use the Actions menu from the main toolbar. See <a href="#">Use Table Views</a> for more information.
View the statuses of interfaces associated with a node	If a node is not completely down, you might want to see which interfaces are down for the selected node. To do so, open the Node form and select the Interfaces tab.
The number of devices that are served by this node.	Select the node you want and access the Layer 2 or Layer 3 Neighbor View using the Actions menu.


## Non-Normal Router Redundancy Group View (NNMi Advanced)

**Tip:** See ["Router Redundancy Group Form \(NNMi Advanced\)" \(on page 79\)](#) for more details about the Router Redundancy Group attributes that appear in this view's column headings.

Your network administrator might have set up groups of redundant routers to help ensure that information packets reach their intended destination. When monitoring your network, use the Non-Normal Router Redundancy Group view to see those router groups whose status is other than Normal. This means there is a problem with one or more interfaces or IP addresses on the routers in the router groups.

For each redundant routers group displayed in the view, you can identify the Router Redundancy Group status, Router Redundancy Group name, the Router Redundancy Group protocol (for example, HSRP), and the date the Router Redundancy Group status was last modified.

#### To see the incidents related to a Router Redundancy Group:

1. Click the  Open icon that precedes the Router Redundancy Group of interest to open the form.
2. Select the **Incidents** tab.

#### To view the members that belong to this group:

Click the  Open icon that precedes the Router Redundancy Group of interest to open the form.

On the **Router Router Redundancy Members** tab, you should see a table view of the nodes and interfaces that belong to the selected Router Redundancy Group.

#### Related Topics

["Router Redundancy Group View \(NNMi Advanced\)" \(on page 24\)](#)

["Router Redundancy Group Form \(NNMi Advanced\)" \(on page 79\)](#)

["Router Redundancy Group View \(NNMi Advanced\)" \(on page 24\)](#)

## Not Responding Address View

**Tip:** See ["IP Address Form" \(on page 73\)](#) for more details about the node attributes that appear in this view's column headings.

The **Not Responding Address** view in the **Monitoring** workspace is useful for identifying all of the addresses whose state is **Not Responding**. A **Not Responding** state indicates that the address is not responding to ICMP ping.

**Note:** Because all addresses in this view have a state of **Not Responding**, the **State** column is not displayed in this view.

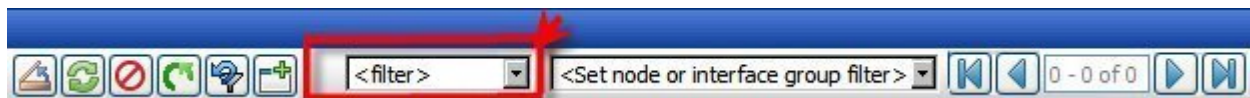
For each address displayed in the view, you can identify the status, address, associated node Name value (**Hosted On Node**), interface, the subnet prefix (**In Subnet**) and prefix length (**PL**), and any notes included for the IP address.

## Nodes by Status View

**Tip:** See ["Node Form" \(on page 28\)](#) for more details about the node attributes that appear in this view's column headings.

The Nodes by Status view in the Monitoring workspace lets you filter your view by the **Status** value. Examples of **Status** values include **Normal**, **Warning**, **Minor**, **Major**, and **Critical**.

**Note:** By default, NNMi uses the first value in the Quick Filter list. If your view is empty, change the filter value. Here is an example of a Quick Filter list:



If your NNMi administrator set up Node Groups or Interface Groups to identify important elements of your environment, you can filter this view to show only the nodes that need your immediate attention. For example, by using the status and node group filters, you can display all nodes that have a Status value of **Critical** and are related to a certain group of nodes.

**Note:** If you filter your view using multiple filters, NNMi uses the AND operator to combine the filters you have selected. See [Filter a Table View](#) for more information.

For each node displayed, you can view its status, device category, name, hostname, management address, system location (the current value of the sysLocation MIB variable), device profile, the date the node's status was last modified, and any notes that exist for this node.

By default, this view is sorted by the date the node status was last modified (**Status Last Modified**).

## Interfaces by Status View

**Tip:** See "[Interface Form](#)" (on page 60) for more details about the node attributes that appear in this view's column headings.

The **Interface by Status** view lets you filter your view by the **Status** value. Examples of **Status** values include **Normal**, **Warning**, **Minor**, **Major**, and **Critical**.

You can use this view to help identify the status of the interfaces that you are monitoring. If your network administrator has set up node or interface groups, by using the status and Node Group filters, you can display the status for only your important interfaces.

For each interface displayed, you can view the status, administrative state, the operational state, associated node Name value for the computer on which the interface resides (**Hosted On Node**), the interface name, type, speed, input speed, output speed, the date the status was last modified, an interface description, the ifAlias value, and any related notes.

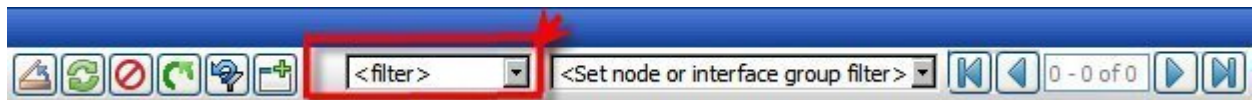
By default, this view is sorted by the date the interface status was last modified (**Status Last Modified**).

## Interfaces by Administrative State View

**Tip:** See "[Interface Form](#)" (on page 60) for more details about the interface attributes that appear in this view's column headings.

The **Interface by Administrative State** view lets you filter your view by the administrative state value. Examples of **Administrative State** include **Up**, **Down**, and **Testing**.

**Note:** By default, NNMi uses the first value in the Quick Filter list. If your view is empty, change the filter value. Here is an example of a Quick Filter list:



You can use this view to help identify the administrative state of your interfaces. If your network administrator has set up node or interface groups for those nodes or interfaces important to you, by using the administrative state and Node Group filters, you can check the state set by your administrator for each of the interfaces that is important to you. This might be useful for proactively monitoring your network and checking for those interfaces whose state indicates there might be a potential problem.

**Note:** If you filter your view using multiple filters, NNMi uses the AND operator to combine the filters you have selected. See [Filter a Table View](#) for more information.

For each interface displayed, you can view its status, the operational state, associated node Name value for the computer on which the interface resides (**Hosted On Node**), interface name, type, speed, input

speed, output speed, the date the status was last modified, a description of the interface, the ifAlias value, and any notes that exist about the interface.

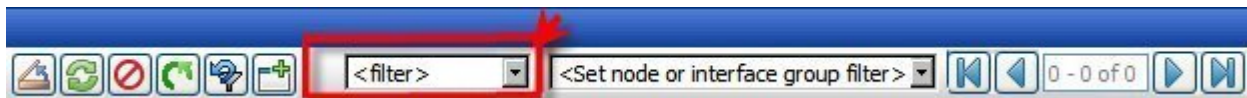
By default, this view is sorted by the date the interface status was last modified (**Status Last Modified**).

## Interfaces by Operational State View

**Tip:** See "[Interface Form](#)" (on page 60) for more details about the interface attributes that appear in this view's column headings.

The **Interface by Operational State** view lets you filter your view by the operational state value. Examples of Operational State include **Up**, **Down**, and **Testing**.

**Note:** By default, NNMi uses the first value in the Quick Filter list. If your view is empty, change the filter value. Here is an example of a Quick Filter list:



You can use this view to help identify the operational state of your interfaces. If your network administrator has set up node or interface groups for those nodes or interfaces important to you, by using the operational state and Node Group filters, you can check the operational state for each of the interfaces that is important to you. This might be useful for proactively monitoring your network and checking for those interfaces whose state indicates there might be a potential problem.

**Note:** If you filter your view using multiple filters, NNMi uses the AND operator to combine the filters you have selected. See [Filter a Table View](#) for more information.

For each interface displayed, you can view its status, the administrative state, associated node Name value of the computer on which the interface resides (**Hosted On Node**), the interface name, type, speed, input speed, output speed, the date the status was last modified, a description of the interface, the ifAlias value, and any notes that exist about the interface.

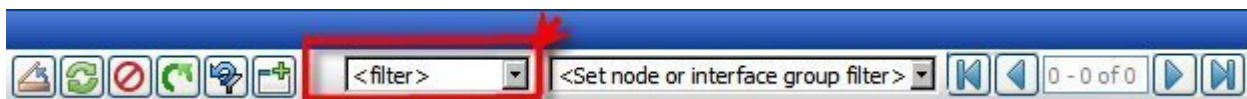
By default, this view is sorted by the date the interface status was last modified (**Status Last Modified**).

## IP Addresses by State View

**Tip:** See "[IP Address Form](#)" (on page 73) for more details about the IP address attributes that appear in this view's column headings.

The IP Addresses by State view in the Monitoring workspace lets you filter your view by the **State** value. Examples of **State** include: **Responding**, **Not Responding**, and **Not Polled**.

**Note:** By default, NNMi uses the first value in the Quick Filter list. If your view is empty, change the filter value. Here is an example of a Quick Filter list:



You can use this view to help identify the state of your IP addresses. If your network administrator has set up node or interface groups for those nodes or interfaces important to you, by using the state and node or interface group filters, you can check the state for only the important addresses.

**Note:** If you filter your view using additional filters, such as Node Groups, NNMi uses the AND operator to combine the filters you have selected. See [Filter a Table View](#) for more information.

For each address displayed in the view, you can see its status, address, the name of the pertinent interface, associated node Name value (**Hosted On Node**), the subnet in which the address is contained, the subnet prefix length (**PL**), the date the status of the address was most recently modified, and any notes included about the IP address.

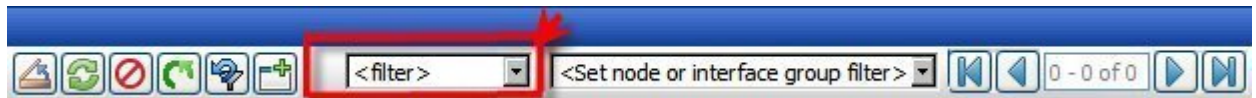
## Component by Status View

**Tip:** See "[Node Form](#)" (on page 28) for more details about the attributes that appear in this view's column headings.

Use the Component by Status view in the Monitoring workspace to help identify the status of node components. Examples of node components include temperature, fan, and memory.

This view lets you filter your view by the **Status** value. Examples of **Status** include: **Critical**, **Warning**, **Major**, **Minor**, and **No Status**.

**Note:** By default, NNMi uses the first value in the Quick Filter list. If your view is empty, change the filter value. Here is an example of a Quick Filter list:



If your network administrator has set up node or interface groups for those nodes or interfaces important to you, by using the status and node or interface group filters, you can check the status for the components for only the important nodes.

**Note:** If you filter your view using additional filters, such as Node Groups, NNMi uses the AND operator to combine the filters you have selected. See [Filter a Table View](#) for more information.

For each component displayed, you can see its status, name, type, and the node on which it resides.

## Interface Performance View (NNM iSPI Performance for Metrics)

(*NNM iSPI Performance for Metrics*) Data appears in this view only if the NNM iSPI Performance for Metrics software is installed and your NNMi administrator enables performance monitoring.

The interface performance view helps you identify the over- and under-utilized interfaces for the nodes in your managed network. Sort this view by Hosted On Node to help you identify potential problem nodes that are over utilized.

If your network administrator has set up node or interface groups for those nodes or interfaces important to you, you can check the interface status for each interface that is important to you. This might be useful for proactively monitoring your network and checking for those interfaces whose input or output utilization, error, or discard rate indicate there might be a potential problem.

**Note:** If you filter your view using multiple filters, NNMi uses the AND operator to combine the filters you have selected. See [Filter a Table View](#) for more information.

For each interface displayed, you can view its input and output utilization rates, input and output error rates, input and output discard rates, associated node Name value of the computer on which the interface resides (**Hosted On Node**), the interface name, speed, input speed, output speed, and any notes that exist about the interface.

**Tip:** See "[Interface Form](#)" (on page 60) for more details about the interface attributes that appear in this view's column headings.

## Node Groups View (Monitoring)

**Tip:** See "[Node Group Form](#)" (on page 88) for more details about the Node Group attributes that appear in this view's column headings.

When monitoring your network, you might be interested in only viewing information for a particular set of nodes. Your network administrator is able to group sets of nodes into node groups. An example node group could be all important Cisco routers, or all routers in a particular building. See [About Node and Interface Groups](#) for more information about how your administrator sets up node groups. See [Filter by Node or Interface Group](#) for more information about filtering views using node and interface groups.

To find the definition for a particular Node Group filter, navigate to the Inventory workspace, and select the Node Groups view.

For each node group displayed in the view, you can identify the node group status, name, whether the node group appears in the filter list for node and interface views, whether the node group is available as a filter in the NNM iSPI Performance for Metrics software, and any notes about the node group.

## Monitor with Map Views

NNMi provides three kinds of map views that show a graphical representation of a selected device and the devices connected to it (Layer 2 Neighbor View, Layer 3 Neighbor View, and Path View).


Map views are useful for the following tasks:

- Identify important connector devices, such as a switch that might be a single connection to a main office or campus.
- Identify how many devices are served by a node or interface.
- Identify routing issues.
- Identify network issues between two nodes.

Each node on the map is represented by a map symbol. Each map symbol has a background shape and a foreground image. The background shape conveys two pieces of information:

- The type of device indicated by shape. See [About Map Symbols](#).
- The most recent health status represented by the background color. See [About Status Colors](#).

The foreground image assists in identifying the device model. NNMi uses first the Family, then Vendor, and then the Category device profile information to determine the foreground image to be displayed. If there is no image defined for any of these attributes, NNMi displays **\*no\* icon** in the map node.

**Note:** Your NNMi administrator is able to delete nodes and other objects from the NNMi database. Any node that has been deleted appears as a transparent icon on the map until the map is refreshed using the  **Refresh** icon. After **Refresh**, the deleted node is removed from the map. NNMi does not automatically refresh the connectivity or set of nodes in a map view, except on the Network Overview map.

To monitor your network using a network map:

- ["Watch Status Colors"](#) (on page 129)
- ["Determine Problem Scope"](#) (on page 129)
- ["Access Node Details"](#) (on page 130)

**Related Topics:**



## [Use Map Views](#)

["Display the Layer 2 Neighbor View" \(on page 104\)](#)

["Display the Layer 3 Neighbor View" \(on page 112\)](#)









["Path Between Two Nodes that Have IPv4 Addresses" \(on page 114\)](#)

## Watch Status Colors

When monitoring the network using a map view, watch for nodes whose status color is non-normal. The background shapes of the map symbols change color based on the current health status of the represented device.

The following table describes the meaning for each status color that might appear on a map.

### Status Colors

Color	Meaning	Description
	Unknown	Indicates one of the following: <ul style="list-style-type: none"><li>The node was just added to the NNMi database, and health status is not yet calculated.</li><li>The node is unreachable and cannot be polled.</li></ul>
	Normal	Indicates there are no known problems related to the associated object.
	Warning	Indicates there may or may not be a problem related to the associated object.
	Minor	Indicates NNMi has detected problems related to the associated object that require further investigation.
	Major	Indicates NNMi detected problems that could precede a critical situation.
	Critical	Indicates NNMi detected problems that require immediate attention.
	Disabled	Indicates the object is administratively "disabled". (The current value of MIB II ifAdminStatus is "disabled".)
	No Status	Indicates that NNMi monitoring configuration specifically excludes this device. The Status is either not calculated or the device is Not Managed/Out Of Service.

## Determine Problem Scope

Maps are a useful tool for determining the scope of a problem. Scan the map to determine the scope of the problem. For example, look for large clusters of non-normal color icons to determine if there is a large-scale outage.

If your naming scheme is based on node location, you might also be able to determine if the problem is isolated to a particular site or store.

## Access a Problem Device

Using NNMi's **Actions** menu you can access the following commonly used tools to investigate device access and configuration information:

- Verify that the node can be reached by using ping, see ["Test Node Access \(Ping\)" \(on page 206\)](#).
- Launch telnet to access the device and determine more information, see ["Establish Contact with a Node \(telnet\)" \(on page 207\)](#).
- Use traceroute to view traffic paths, see ["Find the Route \(traceroute\)" \(on page 206\)](#).

**Note:** Access to these commands depends on the NNMi role to which you are assigned. If you are unable to access an action, contact your NNMi administrator.


## Access Node Details

Select any node symbol on the map, and display all of the information related to that specified node. The Node form is useful for troubleshooting purposes:

- List of the conclusions that led to the current status, and information about status calculations for the node over time.
- Status of each interface contained in the node. For example, if the node is not completely down, you might want to see which interfaces are down.
- Status of each address associated with this node.
- System contact information.
- All of the incidents associated with the node.

NNMi also provides a Quick View that displays a small subset of information about a selected object.

### To view all details associated with a map object:

1. In a map view, select the object.
2. Click the  Open icon in the menu bar.
3. The form displays, containing details of all information related to the object.
4. View or edit the details of the selected object.

### To access the Quick View for a map object:

1. Using your mouse, hover over the object of interest.  
The Quick View window displays, containing a read-only subset of details about the object.
2. To close the Quick View, move your mouse away from the object.

### Related Topics:

["Node Form" \(on page 28\)](#)

["Interface Form" \(on page 60\)](#)



["IP Address Form" \(on page 73\)](#)

## Access All Related Incidents

If you are using a map view to monitor your network, there are times when you might want to switch to an incident view for more information. Information available from an incident view includes the first time a

notification was received, the description of the problem (for example, **Node Down** or **Address Not Responding**), and the incident category. The incident category helps to identify the type of problem, such as fault, performance, or security.

**To display all incidents related to an object on a map:**

1. Click to select the node or interface of interest.
2. Click the  Open icon to open the form.
3. Select the **Incidents** tab.
4. The incidents table includes all incidents associated with the node or interface. Click the  Open icon in the row representing the incident that you want to examine. See "[Incident Form](#)" ([on page 134](#)).

**Related Topics:**

[Using Views to Display Data](#)

[Working with Objects](#)

[Use Table Views](#)

## Monitoring Incidents for Problems

**Tip:** See "[Incident Form](#)" (on page 134) for more details about the Incident attributes that appear in an incident's view column headings.

NNMi actively notifies you when an important event occurs. The event is reflected by a change of background color of a node in a network map and is reported through incident views.

Many services (background processes) within NNMi gather information and generate NNMi incidents. In addition, an SNMP agent might send information to NNMi. For example, an SNMP agent detects that a managed critical server is overheating and about to fail. The SNMP agent forwards a trap to NNMi.




Incidents might also be reporting on information that was requested by NNMi. For example, NNMi might generate an "Address Not Responding" incident after using ICMP to check whether communication channels are open to a device (using ping).

For most incident views displayed, you can identify an incident's overall severity (**Normal**, **Warning**, **Minor**, **Major**, **Critical**, and **Unknown**), lifecycle state, source node, source object, and its message.

**Note:** Some incidents may have a value of **<none>** for the source object or source node. This happens when the source node or object cannot be resolved. For example, an incident that is being forwarded from an NNM 6.x or 7.x management station has a source node value of **<none>**. An SNMP trap whose source is not monitored might be displayed as **<none>**.

The following table describes the severity icons used by NNMi.

### Incident Severity Icons

Icon	Meaning	Icon	Meaning	Icon	Meaning	Icon	Meaning
	Normal		Minor		Critical		Disabled
	Warning		Major		Unknown		No Status

**Note:** NNMi provides management mode attributes that determine whether a node, interface, or address is discovered and monitored. Your administrator is able to set some of these management mode attribute values. Any object whose management mode is set so that it is no longer discovered and monitored might still have incidents associated with it that existed before the object was no longer managed. To check whether a node associated with an incident is being managed, open the form for the incident and then open the form for the source node associated with the incident. See [Working with Objects](#) for more information.

Incident views are useful for quickly identifying items described in the following table.

### Incident View Uses

Use	Description
Identify potential or current problems	Within a view, each incident has a corresponding icon that indicates its severity so that you are immediately notified of potential or current problems. You can filter incidents so that you only view incidents whose severity is Critical or you can choose to filter incidents to view all incidents whose severity is greater than Normal.
Identify problem nodes	You can sort incidents by node to help you quickly identify the problem nodes.
Determine	You can sort an incident view by description so that you are able to see all incidents reporting a node or interface that is disabled or otherwise unavailable.

the cause of the problem	You can also use the child incidents attribute to view all of the incidents that are a result of the root cause problem reported.
Determine historical information	<p>You can sort your incidents by notification date to determine whether a group of nodes went down within a specified time frame.</p> <p>You can also filter your list of incidents according to notification date to view only those incidents received within the last hour.</p> <p>To track historical information for a specific node, sort your incidents by First Occurrence. Then, filter your view by node Name. This lets you view a chronological list of the kinds of errors (indicated by Origin) that have occurred for the current node.</p> <p>You can then open the Incident form to use the child incidents attribute to view all of the incidents that are a result of the root cause problem reported.</p>
Identify only the important incidents to you	You can filter an incident view so that you see only those incidents of interest. For example, you might filter incidents so that you only view incidents whose status is Critical or only those incidents assigned to you. You can also view only those incident associated with a Node Group. Your NNMi administrator creates node groups. For example, your NNMi administrator might choose to group all of your important Cisco routers into a node group. See <a href="#">Node/ Interface Group Filters</a> for more information.

Your NNMi administrator can define the format of incident messages so they are most useful to you and your team.

Your team can use the Notes attribute of the incident views to notify everyone else about which issues are being covered.

#### Tasks Performed from an Incident View

You can perform the following tasks from an incident view:

["Organize Your Incidents" \(on page 133\)](#)

["Own Incidents" \(on page 149\)](#)

["Assign Incidents" \(on page 150\)](#)

["Unassign Incidents" \(on page 150\)](#)

["Keep Your Incidents Up to Date" \(on page 151\)](#)

["Track an Incident's Progress" \(on page 157\)](#)

["Display a Map from an Incident" \(on page 158\)](#)

#### Related Topics:

["Incident Views Provided by NNMi" \(on page 159\)](#)

## Organize Your Incidents

You can organize your incidents in one of three ways:

1. Sort them according to the column of interest. For example, you might want to sort your incidents by status.

2. Filter them according to the values for a particular column or attribute. For example, filtering by status lets you filter out the status values that are not of interest to you. Filtering by the **Assigned To** attribute lets you view only the incidents assigned to you.
3. Filter them according to a Node Group. Your network administrator is able to group sets of nodes into Node Groups. An example Node Group could be all important Cisco routers, or all routers in a particular building. See [Node/Interface Group Filters](#) for more information about filtering a view by Node Group.

**Note:** See the help topic for each incident view for more details about how you might want to sort or filter a specific incident view.

For information about sorting and filtering, see [Use Table Views](#).











## Incident Form











The Incident form provides details for troubleshooting purposes. From this form you can access more details about the [node](#) involved, and the [Source Object](#) attribute provides more information about the interface, IP Address, connection, or SNMP Agent that is contributing to the problem.

If your role allows, you can use this form to update the [priority](#) and [state](#) of the incident, [assign](#) a team member to investigate the problem, or add [notes](#) to communicate solutions or workaround information.

**For information about each tab:**

### Basic Attributes

Attribute	Description
Message	A description of the problem that you want NNMi to display.
Severity	Seriousness that NNMi calculates for the incident. Possible values are:  Normal  Warning  Minor  Major  Critical  See <a href="#">About Status Colors</a> for more information about severity values. <b>Note:</b> The icons are displayed only in table views.
Priority	Used to communicate the urgency of resolving the selected incident. You control this value. NNMi sets this value to null by default. The lower the number the higher the priority. Possible values are:  None  Low  Medium  High  Top














Attribute	Description
	<p><b>Note:</b> The icons are displayed only in table views.</p>
Lifecycle State	<p>Identifies where the incident is in the incident lifecycle. You control this value.</p> <p> <b>Registered</b> – Indicates that an incident arrived in the queue and is stored in the data-base.</p> <p> <b>In Progress</b> – State selected to indicate the incident is being addressed.</p> <p> <b>Completed</b> – State selected to indicate completion of the incident investigation, and implementation of a solution.</p> <p> <b>Closed</b> – Indicates that NNMi confirmed that the problem reported by this Incident is no longer a problem. For example, when you remove an interface from a device, all incidents related to the interface are automatically Closed.</p> <p>See <a href="#">"About the Incident Lifecycle" (on page 154)</a> for more information about <b>Lifecycle State</b>.</p> <p><b>Note:</b> The icons are displayed only in table views.</p>
Source Node	<p>Name assigned to the node associated with the incident. Click the  Lookup icon and select  Quick View or  Open to display more information about the node. See <a href="#">"Node Form" (on page 28)</a> for more information.</p> <p><b>Note:</b> If NNMi is unable to resolve the node, the source node value is <b>&lt;none&gt;</b>. For example, an incident that NNMi receives from a 6.x or 7.x management station, does not have a source node value.</p>
Source Object	<p>Name used to indicate the configuration item that is malfunctioning on the source node. Click the  Lookup icon and select  Quick View or  Open to display more information about the interface, IP address, connection, or SNMP agent.</p> <p><b>Note:</b> All incidents forwarded to NNMi by a 6.x or 7.x NNM management station have a Source Object value of <b>none</b>.</p>
Assigned To	<p>Name of the user to which this incident is assigned. This value must be a valid user name (determined by the NNMi administrator). See <a href="#">"Manage Incident Assignments" (on page 149)</a> for more information.</p>
Notes	<p>Provided for communication among your team (for example, explanations or workarounds). Information might include reasons why the status was changed, what has been done to troubleshoot the problem, or who worked on resolving the incident.</p> <p>Type a maximum of 255 characters. Alpha-numeric, punctuation, spaces, and underline characters are allowed.</p> <p><b>Note:</b> You can sort your incident table views based on this value. Therefore, you might want to include keywords for this attribute value.</p>

## Incident Form: General Tab

















The ["Incident Form" \(on page 134\)](#) provides details for troubleshooting purposes.




**For information about each tab:**

## General Attributes

Attribute	Description
Name	Name of the rule used to configure the incident. This name is initially created by NNMi.
Category	<p>Generated by NNMi to indicate the problem category. Possible values include:</p> <ul style="list-style-type: none"> <li> <b>Accounting</b> - Used to indicate problems related to usage statistics and allocation of costs associated with the billing of time and services provided by devices. This category is not used by NNMi with default configurations, but it is available for incidents you define.</li> <li> <b>Application Status</b> - Indicates there is a problem with the health of the NNMi software. Examples of these kinds of events include license expiration or that a certain NNMi process lost connection to the Process Status Manager.</li> <li> <b>Configuration</b> Indicates there is a problem with the configuration of a managed device; for example there is a physical address mismatch</li> <li> <b>Fault</b> – Indicates a problem with the network, for example Node Down</li> <li> <b>Performance</b> – Indicates a threshold has been exceeded; for example a utility has exceeded 90 percent</li> <li> <b>Security</b> – Indicates there is a problem related to authentication; for example an SNMP authentication failure</li> <li> <b>Status</b> - Often indicates some status change has occurred on a device. For example, when a Cisco device is powered up or powered down.</li> </ul> <p><b>Note:</b> The icons are displayed only in table views.</p>
Family	<p>Used to further categorize the types of incidents that might be generated. Possible values are:</p> <ul style="list-style-type: none"> <li> <b>Address</b> – Indicates the incident is related to an address problem.</li> <li> <b>Aggregated Port</b> – Indicates the incident is related to an link aggregation problem.</li> <li><b>BGP</b> - Indicates the incident is related to a problem with BGP (Border Gateway Protocol). This family is not used by NNMi with default configurations, but it is available for incidents you define.</li> <li><b>Board</b> - Indicates the incident is related to an board problem This family is not used by NNMi with default configurations, but it is available for incidents you define.</li> <li> <b>Chassis</b> – Indicates the incident is related to an board problem This family is not used by NNMi with default configurations, but it is available for incidents you define.</li> <li> <b>Component Health</b> –Indicates the incident is related to Component Health metrics collected by NNMi. See "<a href="#">Node Form: Component Health Tab</a>" (on page 40) for more information about the Component Health metrics collected.</li> <li> <b>Connection</b> – Indicates the incident is related to a problem with one or more connections.</li> <li> <b>Correlation</b> – Indicates the incident has additional incidents correlated beneath it. These incidents are associated with a duplicate count so that you can determine the number of correlated incidents associated with it.</li> </ul>



Attribute	Description
	<p> <b>HSRP</b> – <i>NNMi Advanced</i>. Indicates the incident is related to a Hot Standby Router Protocol problem.</p> <p> <b>Interface</b> – Indicates the incident is related to a problem with one or more interfaces.</p> <p> <b>License</b> - Indicates the incident is related to a licensing problem.</p> <p> <b>Node</b> – Indicates the incident is related to a node problem.</p> <p> <b>OSPF</b> – Indicates the incident is related to an OSPF problem. This family is not used by NNMi with default configurations, but it is available for incidents you define.</p> <p> <b>RAMS</b> – <i>NNMi Advanced</i>. Indicates the incident is related to a Router Analytics Management System problem.</p> <p><b>RMON</b> – Indicates the incident is related to a Remote Monitor (IETF standard, RFC 1757) problem. This family is not used by NNMi with default configurations, but it is available for incidents you define.</p> <p> <b>RRP</b> – <i>NNMi Advanced</i>. Indicates the incident is related to either a Virtual Router Redundancy Protocol (VRRP) or Hot Standby Router Protocol (HSRP) problem.</p> <p><b>STP</b> – Indicates the incident is related to Spanning-Tree Protocol problem. This family is not used by NNMi with default configurations, but it is available for incidents you define.</p> <p><b>Trap Analysis</b> – Indicates the incident is related to an SNMP trap storm.</p> <p> <b>VRRP</b> – <i>NNMi Advanced</i>. Indicates the incident is related to a Virtual Router Redundancy Protocol problem.</p> <p><b>Note:</b> The icons are displayed only in table views.</p>
Origin	<p>Identifies how the incident was generated. Possible values are:</p> <p> <b>Management Software</b> – Indicates the incident was generated by NNMi processes</p> <p> <b>Manually Created</b> – Indicates the incident was created from the user interface.</p> <p> <b>Remotely Generated</b> – Indicates the incident was forwarded from an NNM 6.x or 7.x management station</p> <p> <b>SNMP Trap</b> – Indicates the incident was forwarded from an SNMP Agent</p> <p><b>Note:</b> The icons are displayed only in table views.</p>
Correlation Nature	<p>This incident's contribution to a root-cause calculation, if any. Possible values are:</p> <p> <b>Info</b> - Indicates the incident is informational only. NNMi uses this Correlation Nature to identify Node Up incidents, so that you can view Node Down and Node Up incident pairs.</p> <p> <b>None</b> - Indicates there is no incident correlation for the incident.</p> <p> <b>Root Cause</b> – Indicates the incident is a root cause of the reported problem. For example, node down is a root cause problem.</p> <p> <b>Secondary Root Cause</b> – Indicates the incident is related to root cause, but is not the</p>

Attribute	Description
	<p>primary problem. Secondary root cause incidents often begin as primary root cause incidents. For example, when an interface goes down, it becomes a primary root cause incident. If a connection associated with the interface goes down, the connection down becomes the root cause, and the interface down becomes a Secondary Root Cause.</p> <p> <b>Symptom</b> – Indicates any incidents that were generated from a trap notification related to the root cause incident. For example, a Link Down incident generated from a Link Down trap notification might appear as a <b>Symptom</b> to an Interface Down incident in the root cause incidents view.</p> <p> <b>Stream Correlation</b> – Stream correlations are created as NNMi analyzes events and traps to determine the root cause incident for a problem. Examples of stream correlations include Dedup (duplication of events) Rate (occurrence of events by time), and Pairwise (occurrence of events using incident pairs) correlations.</p> <p> <b>Service Impact</b> - Indicates a relationship between incidents in which a network service is effected by other incidents. For example, an Interface Down incident can effect a Router Redundancy Group that is part of an HSRP service. This Correlation Nature is available for use by NNM iSPIs (HP Smart Plug-ins). See "Help for Administrators" for more information about HP Smart Plug-ins.</p> <p><b>Note:</b> The icons are displayed only in table views.</p>
Duplicate Count	<p>Lists the number of duplicate incidents that NNMi encountered for the selected incident. This number is incremented only in the associated deduplication incident that is generated by NNMi. Deduplication incidents are generated by NNMi to inform the operator of incidents needing attention because they are reoccurring according to the deduplication criteria specified in the incident's deduplication configuration.</p> <p>For example, incidents generated from SNMP traps will not have their deduplication count incremented. If the deduplication criteria is configured for the SNMP trap, NNMi generates an incident specifying that the SNMP trap is reoccurring according to the criteria specified in the incident's associated deduplication configuration. This incident is the one that increments and displays the <b>Duplicate Count</b> value.</p> <p>Note the following:</p> <ul style="list-style-type: none"> <li>• By default, NNMi updates the <b>Duplicate Count</b> every 30 seconds. This interval cannot be changed.</li> <li>• NNMi continues to update the duplicate count regardless of an incident's lifecycle state. For example, if an incident's <b>Lifecycle State</b> is set to <b>Closed</b>, the duplicate count continues to be incremented. See "<a href="#">About the Incident Lifecycle</a>" (on page 154) for more information. This behavior helps you identify situations in which the incident is not yet fixed. Take note if the Duplicate Count is incremented after a lengthy time period has elapsed; this might indicate there is a new problem with the node, interface, or address.</li> <li>• Duplicates are configured by the NNMi administrator using the <b>Incident Configuration</b> form available from the <b>Configuration</b> workspace.</li> </ul>
RCA Active	<p>Used by NNMi to identify whether NNMi considers the incident to be active or inactive. If set to <b>True</b>, the incident is considered to be active. If set to <b>False</b>, the incident is considered to be inactive.</p> <p>NNMi considers an incident to be active when the root cause analysis (RCA) engine is actively evaluating the problem reported by this incident.</p>

Attribute	Description
	<p>NNMi considers an incident to be inactive when NNMi confirmed that the problem reported by this incident is no longer a problem. For example, the device is now functioning properly.</p> <p>NNMi initially sets an incident's <b>RCA Active</b> attribute to True and the <b>Lifecycle State</b> to <b>Registered</b>. When NNMi sets the <b>RCA Active</b> attribute to <b>False</b>, it also sets the incident's <b>Lifecycle State</b> to <b>Closed</b>.</p> <p>Examples of when an incident's <b>RCA Active</b> attribute is set to <b>False</b> include:</p> <ul style="list-style-type: none"> <li>• When an interface goes up, NNMi closes the InterfaceDown incident.</li> <li>• When a node goes up, NNMi closes the NodeDown incident.</li> </ul>

Correlation Notes	<p>Stores notes about the correlation status of the incident.</p> <p>NNMi provides the following information in the <b>Correlation Notes</b> field when it sets an incident's <b>Lifecycle State</b> to <b>Closed</b>:</p> <ul style="list-style-type: none"> <li>• The Conclusion information identifying the reason NNMi changed the incident's Lifecycle State to Closed. For example, NNMi might include an Interface Up Conclusion as the reason an Interface Down incident was closed.</li> </ul> <p><a href="#">Click here for more information about possible Conclusions that cause Down incidents to be closed.</a></p>
-------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

#### Down Incidents and Conclusion Reasons for Closing the Down Incidents

Down Incident	Conclusion Reason for Closing the Down Incident
AddressNotResponding	AddressResponding
BufferOutOfRangeOrMalfunctioning	BufferInRangeAndFunctioning
ConnectionDown	ConnectionUp
ConnectionPartiallyUnresponsive	ConnectionUp
CpuOutOfRangeOrMalfunctioning	CpuInRangeAndFunctioning
CustomPollCritical	CustomPollNormal
CustomPollMajor	CustomPollNormal
CustomPollMinor	CustomPollNormal
CustomPollWarning	CustomPollNormal
FanOutOfRangeOrMalfunctioning	FanInRangeAndFunctioning
InterfaceDisabled	InterfaceEnabled
InterfaceDown	InterfaceUp
MemoryOutOfRangeOrMalfunctioning	MemoryInRangeAndFunctioning
NodeDown	NodeUp
NodeOrConnectionDown	NodeUp
NonSNMPNodeUnresponsive	NodeUp
PowerSupplyOutOfRangeOrMalfunctioning	PowerSupplyInRangeAndFunctioning

Attribute	Description
-----------	-------------

**Down Incidents and Conclusion Reasons for Closing the Down Incidents ( *NNMi Advanced* )**

Down Incident	Conclusion
AggregatorDegraded	AggregatorUp
AggregatorDown	AggregatorUp
AggregatorLinkDegraded	AggregatorLinkUp
AggregatorLinkDown	AggregatorLinkUp
RrgMultiplePrimary	RrgOnePrimary
RrgMultipleSecondary	RrgOneSecondary
RrgMultipleSecondary	RrgManyExpectedSecondary
RrgNoPrimary	RrgOnePrimary
RrgNoSecondary	RrgOneSecondary
RrgNoSecondary	RrgManyExpectedSecondary

**Down Incidents and Conclusion Reasons for Closing the Down Incidents ( *NNM iSPI Performance for Metrics* )**

Down Incident	Conclusion
InterfaceInputDiscardRateHigh	InterfaceInputDiscardRateNominal
InterfaceInputErrorRateHigh	InterfaceInputErrorRateNominal
InterfaceInputUtilizationHigh	InterfaceInputUtilizationNominal
InterfaceInputUtilizationLow	InterfaceInputUtilizationNormal
InterfaceInputUtilizationNone	InterfaceInputUtilizationNominal
InterfaceOutputDiscardRateHigh	InterfaceOutputDiscardRateNominal
InterfaceOutputErrorRateHigh	InterfaceOutputErrorRateNominal
InterfaceOutputUtilizationHigh	InterfaceOutputUtilizationNominal
InterfaceOutputUtilizationLow	InterfaceOutputUtilizationNominal
InterfaceOutputUtilizationNone	InterfaceOutputUtilizationNominal
InterfacePerformanceCritical	InterfacePerformanceClear
InterfacePerformanceWarning	InterfacePerformanceClear

- The time measured between when NNMi detected a problem with one or more network

Attribute	Description
	<p>devices to the time the problem was resolved.</p> <ul style="list-style-type: none"> <li>• The time when NNMi first detected the problem associated with the incident.</li> <li>• The time when NNMi determines the problem associated with the incident is resolved.</li> </ul> <p>NNMi inserts the information in front of any existing information provided.</p> <p><b>Note:</b> NNMi provides Correlation Notes information only when the Causal Engine has analyzed and Closed the incident. Software that is integrated with NNMi might also provide information identifying the reason an incident was closed. Any time an incident is closed manually (for example, by the network operator), NNMi does not provide Correlation Notes information.</p>
First Occurrence Time	Used when suppressing duplicate incidents or when specifying an incident rate. Indicates the time when the duplicate or rate criteria were first met for a set of duplicate incidents or for a set of incidents whose rate criteria were met.
Last Occurrence Time	<p>Used when suppressing duplicate incidents or specifying an incident rate. Indicates the time when the duplicate or rate criteria were last met for a set of duplicate incidents or for a set of incidents whose rate criteria were met.</p> <p>If there are no duplicate incidents or incidents whose rate criteria were met, this date is the same as the First Occurrence Time.</p>
Origin Occurrence Time	The time at which an event occurred that caused the incident to be created.; for example, the time held in the trap.


Attribute	Description
-----------	-------------

## Incident Form: Correlated Parents Tab

The "[Incident Form](#)" (on page 134) provides details for troubleshooting purposes.

For information about each tab:

### Correlated Parents Table


Attribute	Description
Correlated Parents	If the current incident is a child incident, any correlated parent incidents of the child appears in this table view. For example, parent incidents are created when a root cause problem is detected. A Node Down root cause incident is a parent of an Interface Down incident. Therefore, on an Interface Down Incident form, a Node Down incident might appear under the Correlated Parents tab.  Click the  Open icon to view more information about a specific incident.

## Incident Form: Correlated Children Tab

The "[Incident Form](#)" (on page 134) provides details for troubleshooting purposes.

For information about each tab:

### Correlated Children Table


Attribute	Description
Correlated Children	If the current incident is a parent incident, any correlated child incident of the parent appears in this table view. For example, an Interface Down incident would be correlated as a child under a Node Down root cause incident. Therefore, on a Node Down incident form, an Interface Down incident would appear on the Correlated Children tab.  Click the  Open icon to view more information about a specific incident.

## Incident Form: Custom Attributes Tab

The "[Incident Form](#)" (on page 134) provides details for troubleshooting purposes.

For information about each tab:



### Custom Attributes Table

Attribute	Description
Custom Incident Attributes	Used by NNMi to add additional information to the incident that NNMi makes available for viewing. Each CIA includes a name, type, and value group that can be populated differently for different types of incidents. Varbind values that accompany SNMP traps are a common use for this attribute.  Click the  Open icon to open the " <a href="#">Custom Incident Attribute Form</a> " (on page 143) and view more information about a specific attribute.

## Custom Incident Attribute Form

The Custom Incident Attributes (CIAs) form provides extended information that NNMi gathered about the incident. For example, if the incident is reporting an SNMP trap, the Varbind values are stored as CIAs. Each CIA includes a name, type, and value group that can be populated differently for different types of incidents.

To view custom incident attribute information:

1. Navigate to the **Incident** form.
  - a. From the workspace navigation panel, select the **Incidents** workspace.
  - b. Select the incident view that contains the incident of interest; for example, **Root Cause Incidents**.
  - c. To open the Incident form, click the  Open icon that precedes the incident whose information you want to view.
2. In the **Incident** form, select the **Custom Attributes** tab.
3. Click the  Open icon that precedes the custom incident attribute row of interest.

See the table below for an explanation of the Name, Type, and Value attributes displayed.

**Note:** All varbind values are stored as CIAs in NNMi.

### Custom Incident Attributes

Attribute	Description
Name	<p>Name used to identify the CIA.</p> <p>For SNMP traps and events forwarded from NNM 6.x or 7.x management stations, the name is the object identifier (oid) of the forwarded trap or event.</p> <p><b>Note:</b> If different varbinds have the same oid, NNMi appends a number to the original oid; for example: 1.2.3.4.5.6.2.7.1_1 and 1.2.3.4.5.6.2.7.1_2</p>
Type	<p>Describes the type of data that is stored for the CIA. Examples of types include:</p> <p><b>Double</b> - Used to describe real numbers; for example 12.3</p> <p><b>Integer</b> - Used for integer numeric values; for example 1, 2, or 3</p> <p><b>String</b> - Used for character values</p> <p><b>Boolean</b> - Used to store true or false values</p> <p><b>Note:</b> All SNMP trap and NNM 6.x or 7.x management station events types begin with <b>asn</b>. If the CIA represents a varbind value, you may view additional types, such as <b>Counter</b>.</p>
Value	<p>For SNMP traps and events forwarded from an NNM 6.x or 7.x management station, the CIA value is the varbind value in the forwarded event or trap. For management events that are generated from NNMi, this value is the CIA value in the incident that was provided by NNMi.</p>

### Custom Incident Attributes Provided by NNMi (for Operators)

NNMi uses custom incident attributes to attach additional information to incidents.

A subset of CIAs are available for any particular incident. Any relevant CIAs are displayed on the [Incident form](#), in the Custom Attributes tab. There are two categories of possible CIAs:

- SNMP trap varbinds identified by the Abstract Syntax Notation value (ASN.1).Varbinds are defined in MIB files that the NNMi administrator can load into NNMi.
- Custom incident attributes provided by NNMi.

The potential custom incident attributes provided by NNMi are described in the table below.

#### Custom Incident Attributes Provided by NNMi

Name	Description
cia.address	SNMP agent address.
cia.eventoid	NNM 6.x/7.x object identifier (oid) for the incident.
cia.incidentDurationMs	The time measured in milliseconds between when NNMi detected a problem with one or more network devices to the time the problem was resolved.  <b>Note:</b> This CIA is used only when NNMi's Causal Engine has analyzed and Closed the incident. Any time an incident is closed manually (for example, by the network operator), NNMi does not include cia.incidentDuration.
cia.reasonClosed	The Conclusion information identifying the reason NNMi changed the incident's Lifecycle State to Closed. For example, NNMi might include an Interface Up Conclusion as the reason an Interface Down incident was closed.  <b>Note:</b> This CIA is used when NNMi's Causal Engine has analyzed and Closed the incident. Software that is integrated with NNMi might also provide values for cia.reasonClosed. Any time an incident is closed manually (for example, by the network operator), NNMi does not include cia.reasonClosed.
cia.remotemgr	Hostname or IP address of the either of the following: <ul style="list-style-type: none"> <li>• NNM 6.x or 7.x management station that is forwarding the event</li> <li>• NNMi 8.x Regional Manager that is forwarding the event</li> </ul>
cia.remotetopoid	Topology identifier (topoid) of the NNM 6.x or 7.x event
cia.snmpoid	SNMP trap object identifier.
cia.timeIncidentDetectedMs	The timestamp in milliseconds when NNMi first detected the problem on the network device associated with the incident.  <b>Note:</b> This CIA is used only when NNMi's Causal Engine has analyzed and Closed the incident.. Any time an incident is closed manually (for example, by the network operator), NNMi does not include cia.timeIncidentDetected.
cia.timeIncidentResolvedMs	The time when NNMi determines the problem on the network device associated with the incident is resolved.  <b>Note:</b> This CIA is used only when NNMi's Causal Engine has analyzed and Closed the incident. Any time an incident is closed manually (for example, by the network operator), NNMi does not include cia.timeIncidentResolved.



*(NNM iSPI Performance for Metrics)* For network performance monitoring, additional custom incident attributes are provided for your use. [Click here for more information.](#)

**Custom Incident Attributes Provided for Thresholding *(NNM iSPI Performance for Metrics)***

Name	Description
cia.thresholdReason	<i>(NNM iSPI Performance for Metrics)</i> Configured thresholds have a value of null.  Unset thresholds have a value of <b>No threshold settings defined.</b>

---

Name	Description
------	-------------

cia.thresholdParameter

(*NNM iSPI Performance for Metrics*) The monitored attribute that is being measured.

Possible performance threshold values for Nodes include:

- CPU 5Sec Utilization  
Percentage of CPU usage in relation to the total amount of CPU available. This percentage is measure at 5-second intervals.
- CPU 1Min Utilization  
Percentage of CPU usage in relation to the total amount of CPU available. This percentage is measured at 1-minute intervals.
- CPU 5Min Utilization  
Percentage of CPU usage in relation to the total amount of CPU available. This percentage is measured at 5-minute intervals.
- Memory Utilization  
Percentage of memory usage in relation to the total amount of memory available.
- Buffer Utilization  
Percentage of buffer usage in relation to the total amount of buffer space available.
- Buffer Miss Rate  
Counter indicating that the number of available buffers in the pool has dropped below the minimum level.
- Buffer Failure Rate  
Percentage value based on the number of buffer failures caused by insufficient memory when trying to create additional buffers.

Possible performance thresholds for Interfaces include:

- Input Utilization  
The total number of incoming octets traversing the interface as a percentage of the total possible number of octets (based on the ifSpeed value). From Interface to Interface, the exact MIB variables queried vary based on interface speed and whether the system supports the high speed counters for interfaces.

Each interface in an Interface Groups has its utilization calculated by taking the total traffic on all administratively up interfaces in the group and dividing that by the total possible bandwidth.

- Output Utilization  
The total number of outbound octets traversing the interface as a percentage of the total possible number of octets (based on the ifSpeed value). From Interface to Interface, the exact MIB variables queried vary based on interface speed and whether the system supports the high speed counters for interfaces.

Each interface in an Interface Group has its utilization calculated by taking the total traffic on all administratively up interfaces in the group and dividing that by the total possible bandwidth.

- Input Error Rate  
Percentage based on the reported change in the number of input packets on the interface and the packet error count. What constitutes an error is system specific, but likely includes such issues

## Related Topics

["Custom Incident Attribute Form" \(on page 143\)](#)

## Incident Form: Diagnostics Tab (NNM iSPI NET)

The ["Incident Form" \(on page 134\)](#) provides details for troubleshooting purposes.

When you access the Incident Form: Diagnostics Tab, you can view the history of all the NNM iSPI Network Engineering Toolset Diagnostic reports that have been run for the incident's Source Node. Diagnostics are sets of automated commands specific to one or more device types, including Cisco routers and switches, Cisco switch/routers, and Nortel switches.

To generate a new instance of these Diagnostics reports, click **Actions** → **Run Diagnostics**.

**For information about each tab:**

### Diagnostics Table

Attribute	Description
Start Time	Date and time NNM iSPI NET created this instance of the Diagnostics report. NNM iSPI NET uses the locale of the client and the date and time from the NNMi management server.
Definition	The name of the NNM iSPI NET Diagnostics report definition.
Status	The current status of this NNM iSPI NET Diagnostics report, such as <i>Running</i> or <i>Complete</i> .
Report	Click this link to open the actual report.  <b>Note:</b> You might be prompted to provide a user name and password to access the Operations Orchestration software. See the <i>NNM iSPI NET Planning and Installation Guide</i> for more information.
Lifecycle State	The Diagnostic runs if the incident is currently set to this Lifecycle State.
Last Update Time	Date and time NNM iSPI NET last updated this instance of the Diagnostics report. NNM iSPI NET uses the locale of the client and the date and time from the NNMi management server.

## Incident Diagnostic Results Form (Flow Run Result) (NNM iSPI NET)

NNM iSPI Network Engineering Toolset automatically prepares diagnostic reports when certain incidents are generated and when using **Actions** → **Run Diagnostics**. This form shows details about the currently selected diagnostic report instance.

**Note:** Because the values on this form are generated by NNM iSPI NET, these attribute values cannot be modified.

See ["Incident Form: Diagnostics Tab \(NNM iSPI NET\)" \(on page 147\)](#) for more information:

### Diagnostic Results Details

Attribute	Description
Start Time	The time that NNM iSPI NET created the selected diagnostic report instance.

Attribute	Description
Definition	The name of the flow as defined in NNM iSPI NET.
Status	<p>The current status of this NNM iSPI NET Diagnostics report. Possible values include:</p> <p><b>New</b> - The Diagnostic is in the queue, but is not yet running</p> <p><b>In Progress</b> - The Diagnostic has been submitted and is not finished running</p> <p><b>Completed</b> - The Diagnostic has finished running</p> <p><b>Not Submitted</b> - An error condition prevented the Diagnostic from being submitted</p> <p><b>Timed Out</b> - NNMi was unable to submit or run the Diagnostic due to a time out error. The time out limit for submitting a Diagnostic is one hour. The time out limit for running a Diagnostic is four hours.</p> <p>Example error conditions include the following:</p> <ul style="list-style-type: none"> <li>• The number of Diagnostics in the queue might prevent NNMI from submitting the Diagnostic.</li> <li>• A configuration error, such as an incorrect user name or password, might prevent NNMI from accessing the required Operations Orchestration server.</li> </ul> <p>Contact your NNMi administrator for Diagnostic log file information.</p>
Report	NNM iSPI NET uses this text string to display the selected instance of the diagnostics report in a browser window.
Lifecycle State	<p>The Diagnostic runs if the incident is currently set to this Lifecycle State.</p> <p>Possible values include:</p> <ul style="list-style-type: none"> <li>• Registered</li> <li>• In Progress</li> <li>• Completed</li> <li>• Closed</li> </ul> <p>See <a href="#">About the Incident Lifecycle</a> for more information about Lifecycle State.</p> <p>When the Incident is set to this Lifecycle State, the selected Diagnostics (Flow Definitions) is automatically run on each applicable Source Node in the specified Node Group.</p>
Last Update Time	Date and time NNM iSPI NET last updated this instance of the Diagnostics report. NNM iSPI NET uses the locale of the client and the date and time from the NNMi management server.

## Incident Form: Registration Tab

The "[Incident Form](#)" (on page 134) provides details for troubleshooting purposes.

**For information about each tab:**

### Registration

Attribute	Description
Created	Date and time the selected object instance was created. NNM uses the locale of the client and the date and time from the NNMi management server.

Attribute	Description
Last Modified	Date the selected object instance was last modified. NNM uses the locale of the client and the date and time from the NNMi management server.

## Manage Incident Assignments

One of the first things to do with an incident is to assign it to yourself or to another operator. The following table displays the ways you can assign or un-assign an incident and the NNMi user role that is required for each.

### Tasks Related to Assigning Incidents

Task	How	Required Minimum NNMi User Role
Own an incident	Select an incident and use <b>Actions</b> → <b>Own Incident</b> . See <a href="#">"Own Incidents" (on page 149)</a> for more information.	Level 1 Operator
Assign an incident to someone else	There are two ways to assign an incident to someone else (see <a href="#">"Assign Incidents" (on page 150)</a> for more information): <ul style="list-style-type: none"> <li>From any Incident view, select one or more Incidents and use <b>Actions</b> → <b>Assign Incident</b>.</li> <li>From an Incident form, use <b>Actions</b> → <b>Assign Incident</b>.</li> </ul>	Level 1 Operator
Un-assign an incident	Select an incident and use <b>Actions</b> → <b>Unassign Incident</b> . See <a href="#">"Unassign Incidents" (on page 150)</a> for more information.	Level 1 Operator

## Own Incidents

NNMi lets you own incidents. When you specify that you want to own an incident, the incident is assigned to you.

### To own one or more incidents:

- Navigate to the incident view of interest.
  - From the workspace navigation panel, select the **Incident Management** or **Incident Browsing** workspace.
  - Select the incident view of interest; for example **Unassigned Open Key Incidents**.
- Click the  selection box that precedes each incident you want to own.
- Select **Actions** → **Own Incident**.

Your user name appears in the **Assigned To** column in any incident views that include the incident.




**Note:** If you are using the **Unassigned Open Key Incidents** view, the incident is removed from the view because it is no longer unassigned.

As an operator you are able to view incidents assigned to yourself and to others. If you want to view only those incidents assigned to or owned by you, use the **My Open Incidents** view. See ["My Open Incidents View" \(on page 160\)](#) for more information.

## Assign Incidents

If you are an NNMi user with a Level 1 Operator, Level 2 Operator, or Administrator role, you can assign an incident to yourself or to another operator. If the incident is already assigned to another operator, you can change the assignment or [unassign the incident](#).

### To assign or change assignment for one incident:

1. Navigate to the Incident form of interest.
  - a. From the workspace navigation panel, select the **Incident Management** or **Incident Browsing** workspace.
  - b. Select any Incident view.
  - c. Click the  Open icon that precedes the incident you want to assign.
2. Select **Actions** → **Assign Incident**.
3. Select the user name.
4. Click  **Save** to save your changes or  **Save and Close** to save your changes and exit the form..

The user name you entered or selected appears in the **Assigned To** column in any Incident views that include that incident.

**Note:** If you are using the **Unassigned Open Key Incidents** view, the incident is removed from the view because it is no longer unassigned. See "[Unassigned Open Key Incidents View](#)" (on page 163) for more information.

### To assign or change assignment for multiple incidents:

1. Navigate to the Incident view of interest.
  - a. From the workspace navigation panel, select the **Incident Management** or **Incident Browsing** workspace.
  - b. Select any Incident view.
2. Click the  selection box that precedes each incident you want to assign.
3. Select **Actions** → **Assign Incident**.
4. Select the user name.




The user name you selected appears in the **Assigned To** column in any Incident views that include those incidents.

**Note:** If you are using the **Unassigned Open Key Incidents** view, the incident is removed from the view because it is no longer unassigned. See "[Unassigned Open Key Incidents View](#)" (on page 163) for more information.

## Unassign Incidents

If you are an NNMi user with a user role of Level 1 Operator, Level2 Operator, or Administrator, you can unassign an incident for yourself or for another user.

**To unassign one Incident:**

1. Navigate to the incident form of interest.
  - a. From the workspace navigation panel, select the **Incident Management** or **Incident Browsing** workspace.
  - b. Select any incident view.
  - c. Click the  Open icon that precedes the incident you want to unassign.
2. Select **Actions** → **Unassign Incident**.
3. Click  **Save** to save your changes or  **Save and Close** to save your changes and exit the form..

The **Assigned To** column is empty in any incident views that include that incident.

**Note:** The incident is added to the **Unassigned Open Key Incidents** view. See "[Unassigned Open Key Incidents View](#)" (on page 163) for more information.

**To unassign multiple Incidents:**

1. Navigate to the incident view of interest.
  - a. From the workspace navigation panel, select the **Incident Management** or **Incident Browsing** workspace.
  - b. Select any incident view.
2. Click the  selection box that precedes each incident you want to unassign.
3. Select **Actions** → **Unassign Incident**.

The **Assigned To** column is empty in any incident views that include that incident.

**Note:** The incident is added to the **Unassigned Open Key Incidents** view. See "[Unassigned Open Key Incidents View](#)" (on page 163) for more information.



## Keep Your Incidents Up to Date

NNMi provides the **Notes** attribute to help you keep your incident information up-to-date. Use the **Notes** field to explain steps that were taken to date to troubleshoot the problem, workarounds, solutions, and ownership information.

**To update an incident:**

1. If you do not have an incident open, from the Workspace navigation panel, select the incident view you want to open; for example **Open Key Incidents**.
2. From the incident view, open the incident you want to update.
3. Type the annotations that you want to be displayed within the **Notes** field. Type a maximum of 255 characters. Alpha-numeric, punctuation, spaces, and underline characters are allowed.
4. If you need more space to type in your information, click the **Notes** label, and type the information into the window that appears.

**Note:** NNMi might add information to the **Correlation Notes** field to explain why an incident **Life-cycle State** was changed to **Closed**.

- From the main menu, click  **Save** to save your changes or  **Save and Close** to save your changes and exit the form.

You also want to keep your incident lifecycle information up-to-date. See ["Track an Incident's Progress" \(on page 157\)](#) for more information.

NNMi provides the following information in the **Correlation Notes** field when it sets an incident's **Lifecycle State to Closed**:

- The Conclusion information identifying the reason NNMi changed the incident's Lifecycle State to Closed. For example, NNMi might include an Interface Up Conclusion as the reason an Interface Down incident was closed.

Click here for more information about possible Conclusions that cause Down incidents to be closed.

#### Down Incidents and Conclusion Reasons for Closing the Down Incidents

Down Incident	Conclusion Reason for Closing the Down Incident
AddressNotResponding	AddressResponding
BufferOutOfRangeOrMalfunctioning	BufferInRangeAndFunctioning
ConnectionDown	ConnectionUp
ConnectionPartiallyUnresponsive	ConnectionUp
CpuOutOfRangeOrMalfunctioning	CpuInRangeAndFunctioning
CustomPollCritical	CustomPollNormal
CustomPollMajor	CustomPollNormal
CustomPollMinor	CustomPollNormal
CustomPollWarning	CustomPollNormal
FanOutOfRangeOrMalfunctioning	FanInRangeAndFunctioning
InterfaceDisabled	InterfaceEnabled
InterfaceDown	InterfaceUp
MemoryOutOfRangeOrMalfunctioning	MemoryInRangeAndFunctioning
NodeDown	NodeUp
NodeOrConnectionDown	NodeUp
NonSNMPNodeUnresponsive	NodeUp
PowerSupplyOutOfRangeOrMalfunctioning	PowerSupplyInRangeAndFunctioning
VoltageOutOfRangeOrMalfunctioning	VoltageInRangeAndFunctioning
TemperatureOutOfRangeOrMalfunctioning	TemperatureInRangeAndFunctioning



**Down Incidents and Conclusion Reasons for Closing the Down Incidents (NNMi Advanced )**

Down Incident	Conclusion
AggregatorDegraded	AggregatorUp
AggregatorDown	AggregatorUp
AggregatorLinkDegraded	AggregatorLinkUp
AggregatorLinkDown	AggregatorLinkUp
RrgMultiplePrimary	RrgOnePrimary
RrgMultipleSecondary	RrgOneSecondary
RrgMultipleSecondary	RrgManyExpectedSecondary
RrgNoPrimary	RrgOnePrimary
RrgNoSecondary	RrgOneSecondary
RrgNoSecondary	RrgManyExpectedSecondary

**Down Incidents and Conclusion Reasons for Closing the Down Incidents (NNM iSPI Performance for Metrics)**

Down Incident	Conclusion
InterfaceInputDiscardRateHigh	InterfaceInputDiscardRateNominal
InterfaceInputErrorRateHigh	InterfaceInputErrorRateNominal
InterfaceInputUtilizationHigh	InterfaceInputUtilizationNominal
InterfaceInputUtilizationLow	InterfaceInputUtilizationNormal
InterfaceInputUtilizationNone	InterfaceInputUtilizationNominal
InterfaceOutputDiscardRateHigh	InterfaceOutputDiscardRateNominal
InterfaceOutputErrorRateHigh	InterfaceOutputErrorRateNominal
InterfaceOutputUtilizationHigh	InterfaceOutputUtilizationNominal
InterfaceOutputUtilizationLow	InterfaceOutputUtilizationNominal
InterfaceOutputUtilizationNone	InterfaceOutputUtilizationNominal
InterfacePerformanceCritical	InterfacePerformanceClear
InterfacePerformanceWarning	InterfacePerformanceClear

- The time measured between when NNMi detected a problem with one or more network devices to the time the problem was resolved.
- The time when NNMi first detected the problem associated with the incident.
- The time when NNMi determines the problem associated with the incident is resolved.

NNMi inserts the information in front of any existing information provided.

**Note:** NNMi provides Correlation Notes information only when the Causal Engine has analyzed and Closed the incident. Software that is integrated with NNMi might also provide information identifying the reason an incident was closed. Any time an incident is closed manually (for example, by the network operator), NNMi does not provide Correlation Notes information.

## About the Incident Lifecycle

NNMi provides the Lifecycle State attribute to help you track an incident's progress. See ["Track an Incident's Progress" \(on page 157\)](#) for more information about possible lifecycle states.

In some cases, NNMi updates an incident's Lifecycle State for you. For example, NNMi initially sets an incident's Lifecycle State to **Registered**. It also sets an incident's Lifecycle State to **Closed**. NNMi considers an incident to be **Closed** when NNMi has confirmed that the problem reported by this incident is no longer a problem. For example, the device is now functioning properly. Examples of when NNMi sets an incident Lifecycle State to **Closed** include:

- When an interface goes up, NNMi closes the Interface Down incident.
- When a node goes up, NNMi closes the Node Down incident.

NNMi provides the following information in the **Correlation Notes** field when it sets an incident's **Lifecycle State** to **Closed**:

- The Conclusion information identifying the reason NNMi changed the incident's Lifecycle State to Closed. For example, NNMi might include an Interface Up Conclusion as the reason an Interface Down incident was closed.

[Click here](#) for more information about possible Conclusions that cause Down incidents to be closed.

### Down Incidents and Conclusion Reasons for Closing the Down Incidents

Down Incident	Conclusion Reason for Closing the Down Incident
AddressNotResponding	AddressResponding
BufferOutOfRangeOrMalfunctioning	BufferInRangeAndFunctioning
ConnectionDown	ConnectionUp
ConnectionPartiallyUnresponsive	ConnectionUp
CpuOutOfRangeOrMalfunctioning	CpuInRangeAndFunctioning
CustomPollCritical	CustomPollNormal
CustomPollMajor	CustomPollNormal

Down Incident	Conclusion Reason for Closing the Down Incident
CustomPollMinor	CustomPollNormal
CustomPollWarning	CustomPollNormal
FanOutOfRangeOrMalfunctioning	FanInRangeAndFunctioning
InterfaceDisabled	InterfaceEnabled
InterfaceDown	InterfaceUp
MemoryOutOfRangeOrMalfunctioning	MemoryInRangeAndFunctioning
NodeDown	NodeUp
NodeOrConnectionDown	NodeUp
NonSNMPNodeUnresponsive	NodeUp
PowerSupplyOutOfRangeOrMalfunctioning	PowerSupplyInRangeAndFunctioning
VoltageOutOfRangeOrMalfunctioning	VoltageInRangeAndFunctioning
TemperatureOutOfRangeOrMalfunctioning	TemperatureInRangeAndFunctioning

**Down Incidents and Conclusion Reasons for Closing the Down Incidents (NNMi Advanced )**

Down Incident	Conclusion
AggregatorDegraded	AggregatorUp
AggregatorDown	AggregatorUp
AggregatorLinkDegraded	AggregatorLinkUp
AggregatorLinkDown	AggregatorLinkUp
RrgMultiplePrimary	RrgOnePrimary
RrgMultipleSecondary	RrgOneSecondary
RrgMultipleSecondary	RrgManyExpectedSecondary
RrgNoPrimary	RrgOnePrimary
RrgNoSecondary	RrgOneSecondary
RrgNoSecondary	RrgManyExpectedSecondary

**Down Incidents and Conclusion Reasons for Closing the Down Incidents (NNM iSPI Performance for Metrics)**

Down Incident	Conclusion
InterfaceInputDiscardRateHigh	InterfaceInputDiscardRateNominal
InterfaceInputErrorRateHigh	InterfaceInputErrorRateNominal
InterfaceInputUtilizationHigh	InterfaceInputUtilizationNominal
InterfaceInputUtilizationLow	InterfaceInputUtilizationNormal
InterfaceInputUtilizationNone	InterfaceInputUtilizationNominal
InterfaceOutputDiscardRateHigh	InterfaceOutputDiscardRateNominal
InterfaceOutputErrorRateHigh	InterfaceOutputErrorRateNominal
InterfaceOutputUtilizationHigh	InterfaceOutputUtilizationNominal
InterfaceOutputUtilizationLow	InterfaceOutputUtilizationNominal
InterfaceOutputUtilizationNone	InterfaceOutputUtilizationNominal
InterfacePerformanceCritical	InterfacePerformanceClear
InterfacePerformanceWarning	InterfacePerformanceClear

- The time measured between when NNMi detected a problem with one or more network devices to the time the problem was resolved.
- The time when NNMi first detected the problem associated with the incident.
- The time when NNMi determines the problem associated with the incident is resolved.

NNMi inserts the information in front of any existing information provided.

**Note:** NNMi provides Correlation Notes information only when the Causal Engine has analyzed and Closed the incident. Software that is integrated with NNMi might also provide information identifying the reason an incident was closed. Any time an incident is closed manually (for example, by the network operator), NNMi does not provide Correlation Notes information.

Another way to help you identify those incidents closed by NNMi is by looking at the RCA Active attribute value. When NNMi considers an incident to be **Closed**, it sets the RCA Active attribute value to **False**. This means NNMi's root cause analysis (RCA) engine is no longer actively evaluating the problem reported by this incident.

**Note:** NNMi continues to update the duplicate count regardless of an incident's Lifecycle State. For example, if an incident's Lifecycle State is set to **Closed**, the Duplicate Count continues to be incremented. This behavior helps you identify situations in which the incident is not yet fixed. Take note if the Duplicate Count is incremented after a lengthy time period has elapsed; this might indicate there is a new problem with the node, interface, or address.

After closing a primary root cause incident, any incidents that are correlated and marked as secondary root cause become primary root cause.

## Track an Incident's Progress

NNMi provides the **Lifecycle State** attribute to help you track an incident's progress. The table below describes each lifecycle category and possible values. Your network administrator might have additional or different guidelines for their use.

### Incident Lifecycle States

Lifecycle State	Description
Registered	Indicates that an incident has arrived in the queue and has been stored in the database.
In Progress	State selected by a user to indicate the incident is being addressed.
Completed	State selected by the user to indicate the incident investigation is complete and a solution has been implemented.
Closed	Indicates that NNMi confirmed that the problem reported by this incident is no longer a problem. For example, when you remove an interface from a device all incidents related to the interface are automatically Closed.

You should know your guidelines for lifecycle states so that you can keep your incidents updated accordingly.


To update your lifecycle state, use the **Actions** menu or a form.

#### To update your lifecycle state using the Actions menu from a view:

1. If you do not have an incident open, from the workspace navigation panel, select the incident view you want to open.
2. From the incident view, click the  selection box that precedes the incident whose lifecycle state you want to change.
3. From the main menu toolbar, select **Actions** and then the lifecycle state you want, for example, **In Progress**.

#### To update your lifecycle state from a form:

1. If you do not have an incident open, from the workspace navigation panel, select the incident view you want to open.
2. From the incident view, open the incident you want to update.  
Under the **Basics** pane, select the lifecycle state you want from the drop-down menu.

From the main menu, click **Save** to save your changes or  **Save and Close** to save your changes and exit the form.

From the form menu, select **Actions** and then the lifecycle state you want. For example, select **Completed**.

The action takes effect immediately. This means you do not have to select **Save**.

After performing an action on a form that modifies the object being viewed, you must refresh the form before you can save any additional changes.

## Display a Map from an Incident

If you are using incident views to monitor your network, there are times when you might want to switch to a map view to determine more information. For example, you might want to view the connectivity for a selected node.

### To display a map from an incident:


1. Select the incident of interest by checking the  selection box that precedes the object information.
2. Select **Actions** → **Node Group Map** in the main toolbar.

Note the following:

- This action displays the lowest level Node Group map to which the Source Node belongs. For example, if the node belongs to a Child Node Group, the Child Node Group displays.
- If the Source Node is a member of more than one Node Group at the lowest level, NNMi prompts you to select the Node Group map you want to display.
- If you select **Node Group Map** and the Source Node is not a member of a Node Group, NNMi informs you that no Node Group map is available.

The map launches based on the source node of the selected incident.

**Note:** If the incident is associated with an Island Node Group, NNMi displays the associated Island Node Group map. See ["Island Node Group Map" \(on page 158\)](#) for more information.

**Note:** The current values of the management mode attributes determine whether NNMi discovers and monitors a node, interface, or address. Your NNMi administrator sets some of these management mode attribute values. Map symbols with the color set to  **No Status** are not currently being monitored.

### Related Topics:

[Use Map Views](#)

["Display the Layer 2 Neighbor View" \(on page 104\)](#)

["Display the Layer 3 Neighbor View" \(on page 112\)](#)

["Path Between Two Nodes that Have IPv4 Addresses" \(on page 114\)](#)

["Node Group Overview Map" \(on page 101\)](#)

["Routers Map" \(on page 103\)](#)

["Switches Map" \(on page 103\)](#)

["Networking Infrastructure Devices Map" \(on page 102\)](#)

## Island Node Group Map

An Island Node Group is a group of connected nodes that NNMi discovers and that are not connected to the rest of the topology. An example of an environment with multiple Island Node Groups is a financial institution or retail store with many branches or stores. Each branch or store might be connected to other branches or stores with a WAN (Wide Area Network) connection. Each branch or store appears as an isolated island of nodes in the NNMi topology.

The Island Node Group map contains the Island Node Group that is the Source Object for the selected incident.

**Note:** Incidents whose Source Object is an Island Node Group include **Remote site** in the incident message.

**To display an Island Node Groups Map from an incident:**

1. Select an incident view from the **Incident Management** or **Incident Browsing** workspace.
2. Check the selection box () that precedes the Island Node Group incident whose map you want to display.
3. Select **Actions** → **Node Group Map**.

**Related Topics**

[Node Group Map Objects](#)

## Incident Views Provided by NNMi

You and your team can easily monitor the posted incidents and take appropriate action to preserve the health of your network. To assist you, NNMi provides the following out-of-the-box views for listing incident information:

- ["My Open Incidents View" \(on page 160\)](#)
- ["Open Key Incidents View" \(on page 161\)](#)
- ["Unassigned Open Key Incidents View" \(on page 163\)](#)
- ["Open Key Incidents by Severity View" \(on page 164\)](#)
- ["Open Key Incidents by Priority View" \(on page 165\)](#)
- ["Open Key Incidents by Category View" \(on page 166\)](#)
- ["Open Key Incidents by Family View" \(on page 167\)](#)
- ["Closed Key Incidents View" \(on page 168\)](#)
- ["Key Incidents by Lifecycle State View" \(on page 169\)](#)
- ["Root Cause Incidents View" \(on page 171\)](#)
- ["Service Impact Incidents View" \(on page 172\)](#)
- ["Stream Correlation Incidents View" \(on page 172\)](#)
- ["Custom Incidents View" \(on page 173\)](#)
- ["NNM 6.x/7.x Events View " \(on page 174\)](#)
- ["NNM 6.x/7.x Events by Category View" \(on page 174\)](#)
- ["SNMP Traps View" \(on page 175\)](#)
- ["SNMP Traps by Family View" \(on page 175\)](#)

The most useful views for proactively monitoring your network for problems are the **Key Incident** views. These views include root cause incidents and their associated symptoms.

NNMi's Causal Engine uses ICMP and SNMP to constantly monitor your network. The Causal Engine uses the data collected from all the devices on your network to determine the root cause of known and potential problems.

**Note:** The **Custom Incidents** view lets you use sorting and filtering to customize additional views while maintaining the out-of-the-box views provided by NNMi. This view includes most of the attributes available for the incident so that you can decide which are most important for you to display. See [Use Table Views](#) for more information about sorting, filtering, and hiding attributes within a view.

For each incident generated, you can view the **Correlated Parents** and **Correlated Children** tab information to assist you in understanding how the problem was detected.

NNMi also enables you to access the following 6.x/7.x features by selecting only incidents generated from 6.x/7.x events: (See for more information.) You cannot access these features for any non-6.x/7.x incidents.

- Actions → NNM 6.x/7.x Neighbor View
- Actions → NNM 6.x/7.x Details
- Actions → NNM 6.x/7.x oww

Other useful tasks from the incident view, include the following:

- ["Display a Map from an Incident" \(on page 158\)](#)
- ["Node Form" \(on page 28\)](#)

#### **Related Topics:**

[Accessing Groups of Views \(Workspaces\)](#)

[About the NNMi Console](#)

## **My Open Incidents View**

**Tip:** See ["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in this view's column headings.

The **My Open Incidents** view displays all of the open incidents that have been assigned to you. This view is useful for identifying the incidents for which you are responsible. It displays all incidents assigned to you whose lifecycle state is **Registered**, **In Progress**, or **Completed**. As with all incident views, you can filter this view by time period. The default time period is **Last Week** so that you can view all of the open incidents assigned to you that have occurred within the last week.

For each incident displayed, you can view its severity, its priority, its lifecycle state (for example **In Progress** or **Completed**), the date and time the incident last occurred, the name of its source node, its source object, its category (for example, **Fault** or **Security**), its family (for example, **Interface** or **Connection**), its origin (for example, Management Software or SNMP Trap), its Correlation Nature (for example, **Symptom** or **Root Cause**), the message used to describe the incident, and any related notes.

See ["Monitoring Incidents for Problems" \(on page 132\)](#) for more information about ways to use incident views.

## **Key Incident Views**

**Tip:** See ["IP Address Form" \(on page 73\)](#) ["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in a root cause incident view's column headings.



The Key Incident views are useful for identifying incidents that are most important to the network Operator and that often require more immediate action. The Key Incidents views includes those incidents whose Correlation Nature is any of the following:

Incident Correlation Nature	Description
None	Indicates there is no incident correlation for this incident.
Root Cause	Indicates the incident that reports the root cause of a problem.
Service Impact	<p>Indicates a relationship between incidents in which a network service is effected by other incidents. By default, NNMi generates Service Impact incidents for Router Redundancy Groups. For example, an Interface Down incident can effect a Router Redundancy Group that is part of an HSRP service. The Service Impact incident helps to identify the service that is affected.</p> <p>This Correlation Nature is available for use by NNM iSPIs (HP Smart Plug-ins). See "Help for Administrators" for more information about HP Smart Plug-ins.</p>

Some Key Incident views are filtered according to lifecycle state values, which can be set by the user. For example, the **Open Key Incidents** view displays the Key Incidents whose lifecycle state value is **Registered**, **In Progress**, or **Completed**. The **Closed Key Incidents** view displays only the Key Incidents whose lifecycle state value is **Closed**. NNMi also provides an **Unassigned Open Key Incidents** view that is filtered using the **Lifecycle State** values of **Registered**, **In Progress**, and **Completed** as well as the **Assigned To** attribute

NNMi provides the following Key Incident views:

- ["Open Key Incidents View" \(on page 161\)](#)
- ["Unassigned Open Key Incidents View" \(on page 163\)](#)
- ["Open Key Incidents by Severity View" \(on page 164\)](#)
- ["Open Key Incidents by Priority View" \(on page 165\)](#)
- ["Open Key Incidents by Category View" \(on page 166\)](#)
- ["Open Key Incidents by Family View" \(on page 167\)](#)
- ["Closed Key Incidents View" \(on page 168\)](#)
- ["Key Incidents by Lifecycle State View" \(on page 169\)](#)

#### Related Topics

[Use Table Views](#)

["Organize Your Incidents" \(on page 133\)](#)

["Monitoring Incidents for Problems" \(on page 132\)](#)

["Display a Map from an Incident" \(on page 158\)](#)

## Open Key Incidents View

**Tip:** See "[Incident Form](#)" ([on page 134](#)) for more details about the incident attributes that appear in this view's column headings.

The **Open Key Incidents** view shows the incidents that are most important to network Operators and that often require more immediate action. This view displays the Key Incidents whose lifecycle state value indicates that the incident has not yet been closed. This view is useful for identifying the Key Incidents that need to be resolved. As with all incident views, you can filter this view by time period. The default time period is **Last Week** so that you can view all of the Key Incidents that have remained open within the last week.

This view includes those incidents whose Correlation Nature is any of the following:

Incident Correlation Nature	Description
None	Indicates there is no incident correlation for this incident.
Root Cause	Indicates the incident that reports the root cause of a problem.
Service Impact	Indicates a relationship between incidents in which a network service is effected by other incidents. By default, NNMi generates Service Impact incidents for Router Redundancy Groups. For example, an Interface Down incident can effect a Router Redundancy Group that is part of an HSRP service. The Service Impact incident helps to identify the service that is affected.  This Correlation Nature is available for use by NNM iSPIs (HP Smart Plug-ins). See "Help for Administrators" for more information about HP Smart Plug-ins.
Stream Correlation	Indicates the correlations that NNMi's event pipeline establishes as it recognizes patterns in the flow of events through the pipeline. Correlations are created as NNMi analyzes events and traps to determine the root cause incident for a problem. Examples of stream correlations include Dedup (duplication of events) and Rate (occurrence of events by time) correlations.

For each incident displayed, you can view its severity, its priority, its lifecycle state (for example **In Progress** or **Closed**), the date and time the incident last occurred, the name of the person to which the incident is assigned, the name of its source node, its source object, its category (for example, **Fault** or **Security**), its family (for example, **Interface** or **Connection**), its origin (for example, **Management Software** or **SNMP Trap**), its **Correlation Nature** (for example, **Root Cause**), the message used to describe the incident, and any related notes.

See "[Monitoring Incidents for Problems](#)" ([on page 132](#)) for more information about ways to use incident views.

You can also access additional views from this one using the Actions menu as described in [Use Table Views](#). One example of an action available from an open root cause incident view is the ability to access a map view of the nodes related to the incident.

### Related Topics

[Use Table Views](#)

["Organize Your Incidents" \(on page 133\)](#)

["Monitoring Incidents for Problems" \(on page 132\)](#)

["Display a Map from an Incident" \(on page 158\)](#)

["Key Incident Views" \(on page 160\)](#)

["Unassigned Open Key Incidents View" \(on page 163\)](#)

["Open Key Incidents by Severity View" \(on page 164\)](#)

["Open Key Incidents by Priority View" \(on page 165\)](#)

["Open Key Incidents by Category View" \(on page 166\)](#)

["Open Key Incidents by Family View" \(on page 167\)](#)

["Closed Key Incidents View" \(on page 168\)](#)

["Key Incidents by Lifecycle State View" \(on page 169\)](#)

## Unassigned Open Key Incidents View

**Tip:** See ["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in this view's column headings.

The **Unassigned Open Key Incident** view displays all of the open unassigned Key Incidents. This view is useful for identifying the Key Incidents that are open and must still be assigned to someone. As with all incident views, you can filter this view by time period. The default time period is **Last Day** so that you can view all of the incidents that have remained unassigned with the last day.

For each incident displayed, you can view its severity, its priority, its lifecycle state (for example **In Progress**), the date and time the incident last occurred, the name of its source node, its source object, its category (for example, **Fault** or **Security**), its family (for example, **Interface** or **Connection**), its origin (for example, **Management Software** or **SNMP Trap**), its Correlation Nature (for example, **Root Cause**), the message used to describe the incident, and any related notes.

See ["Monitoring Incidents for Problems" \(on page 132\)](#) for more information about ways to use incident views.

### Related Topics

#### [Use Table Views](#)

["Organize Your Incidents" \(on page 133\)](#)

["Monitoring Incidents for Problems" \(on page 132\)](#)

["Display a Map from an Incident" \(on page 158\)](#)

["Key Incident Views" \(on page 160\)](#)

["Open Key Incidents View" \(on page 161\)](#)

["Open Key Incidents by Severity View" \(on page 164\)](#)

["Open Key Incidents by Priority View" \(on page 165\)](#)

["Open Key Incidents by Category View" \(on page 166\)](#)

["Open Key Incidents by Family View" \(on page 167\)](#)

["Closed Key Incidents View" \(on page 168\)](#)

["Key Incidents by Lifecycle State View" \(on page 169\)](#)

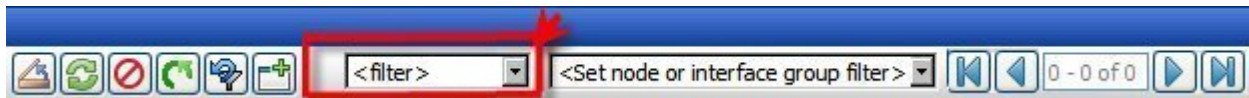
## Open Key Incidents by Severity View

**Tip:** See ["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in this view's column headings

The Open Key Incidents by Severity view lets you filter your view by the Severity value. Possible Severity values include:

- Normal
- Warning
- Minor
- Major
- Critical

**Note:** By default, NNMi uses the first value in the Quick Filter filter list. If your view is empty, change the filter value. Here is an example of a Quick Filter list:



If your NNMi administrator set up Node Groups or Interface Groups to identify important elements of your environment, you can filter this view to show only the incidents that need your immediate attention. For example, by using the severity and node group filters, you can display all incidents that have a Severity value of **Critical** and are related to a certain group of nodes.

As with all incident views, you can filter this view by time period. The default time period is **Last Week** so that you can view all of the open incidents of a specified severity that have occurred within the last week.

**Note:** If you filter your view using multiple filters, NNMi uses the AND operator to combine the filters you have selected. See [Filter a Table View](#) for more information.

For each incident displayed, you can view its priority, its lifecycle state (for example **In Progress** or **Closed**), the date and time the incident last occurred, to whom the incident is assigned, the name of its source node, its source object, its category (for example, **Fault** or **Security**), its family (for example, **Interface** or **Connection**), its origin (for example, **Management Software** or **SNMP Trap**), its Correlation Nature (for example, **Root Cause**), the message used to describe the incident, and any related notes.

### Related Topics

["Key Incident Views" \(on page 160\)](#)

["Organize Your Incidents" \(on page 133\)](#)

["Monitoring Incidents for Problems" \(on page 132\)](#)

["Display a Map from an Incident" \(on page 158\)](#)

["Key Incident Views" \(on page 160\)](#)

["Open Key Incidents View" \(on page 161\)](#)

["Unassigned Open Key Incidents View" \(on page 163\)](#)

["Open Key Incidents by Priority View" \(on page 165\)](#)

["Open Key Incidents by Category View" \(on page 166\)](#)

["Open Key Incidents by Family View" \(on page 167\)](#)

["Closed Key Incidents View" \(on page 168\)](#)

["Key Incidents by Lifecycle State View" \(on page 169\)](#)

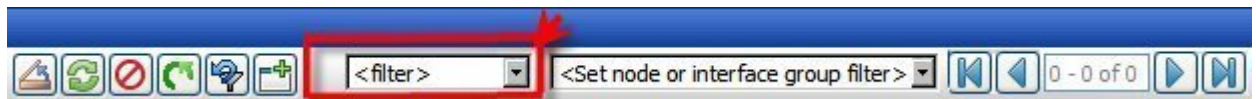
## Open Key Incidents by Priority View

**Tip:** See ["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in this view's column headings.

The **Open Key Incidents by Priority** view lets you filter your view by the Priority value. Possible Priority values include:

- None
- Low
- Medium
- High
- Top

**Note:** By default, NNMi uses the first value in the Quick Filter list. If your view is empty, change the filter value. Here is an example of a Quick Filter list:



If your NNMi administrator set up Node Groups or Interface Groups to identify important elements of your environment, you can filter this view to show only the incidents that need your immediate attention. For example, by using the priority and Node Group filters, you can display all incidents that have a **High** or **Top** priority and are related to a certain group of nodes.

As with all incident views, you can filter this view by time period. The default time period is **Last Week** so that you can view all of the open incidents of a specified priority that have occurred within the last week.

**Note:** If you filter your view using multiple filters, NNMi uses the AND operator to combine the filters you have selected. See [Filter a Table View](#) for more information.

For each incident displayed, you can view its severity, its lifecycle state (for example **In Progress** or **Closed**), the date and time the incident last occurred, to whom the incident is assigned, the name of its source node, its source object, its category (for example, **Fault** or **Security**), its family (for example, **Interface** or **Connection**), its origin (for example, **Management Software** or **SNMP Trap**), its Correlation Nature (for example, **Root Cause**), the message used to describe the incident, and any related notes.

### Related Topics

[Use Table Views](#)

["Organize Your Incidents" \(on page 133\)](#)

["Monitoring Incidents for Problems" \(on page 132\)](#)

["Display a Map from an Incident" \(on page 158\)](#)

["Key Incident Views" \(on page 160\)](#)

["Open Key Incidents View"](#)

["Unassigned Open Key Incidents View" \(on page 163\)](#)

["Open Key Incidents by Severity View" \(on page 164\)](#)["Open Key Incidents by Priority View" \(on page 165\)](#)

["Open Key Incidents by Category View" \(on page 166\)](#)

["Open Key Incidents by Family View" \(on page 167\)](#)

["Closed Key Incidents View" \(on page 168\)](#)

["Key Incidents by Lifecycle State View" \(on page 169\)](#)

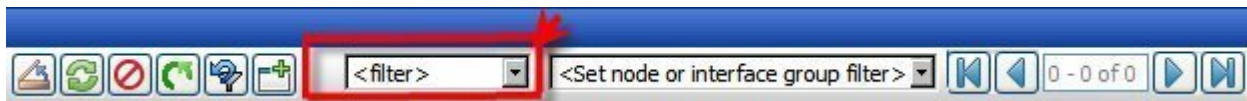
## Open Key Incidents by Category View

**Tip:** See ["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in this view's column headings

The **Open Key Incidents by Category** view lets you filter your view by the Category value. Possible Category values include:

- Accounting
- Application Status
- Fault
- Performance
- Security
- Status

**Note:** By default, NNMi uses the first value in the Quick Filter list. If your view is empty, change the filter value. Here is an example of a Quick Filter list:



You can use this view to help you determine the types of incidents that are in the queue. For example, you might want to look at only incidents related to faults or to performance to help guide you in making troubleshooting decisions.

As with all incident views, you can filter this view by time period. The default time period is **Last Week** so that you can view all of the open incidents by a specified category that have occurred within the last week.

**Note:** If you filter your view using multiple filters, NNMi uses the AND operator to combine the filters you have selected. See [Filter a Table View](#) for more information.

For each incident displayed, you can view its severity, its priority, its lifecycle state (for example **In Progress** or **Closed**), the date and time the incident last occurred, to whom the incident is assigned, the name of its source node, its source object, its family (for example, **Interface** or **Connection**), its origin (for example, **Management Software** or **SNMP Trap**), the message used to describe the incident, and any related notes.

### Related Topics

["Key Incident Views" \(on page 160\)](#)

["Organize Your Incidents" \(on page 133\)](#)

["Monitoring Incidents for Problems" \(on page 132\)](#)

["Display a Map from an Incident" \(on page 158\)](#)

["Key Incident Views" \(on page 160\)](#)

["Open Key Incidents View" \(on page 161\)](#)

["Unassigned Open Key Incidents View" \(on page 163\)](#)

["Open Key Incidents by Severity View" \(on page 164\)"Open Key Incidents by Priority View" \(on page 165\)](#)

["Open Key Incidents by Priority View" \(on page 165\)](#)

["Open Key Incidents by Family View" \(on page 167\)](#)

["Closed Key Incidents View" \(on page 168\)](#)

["Key Incidents by Lifecycle State View" \(on page 169\)](#)

## Open Key Incidents by Family View

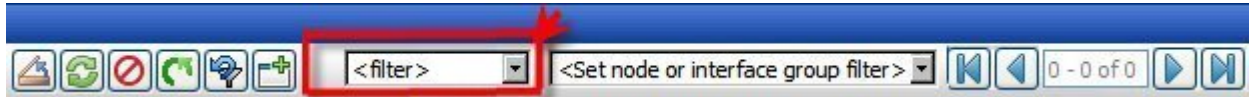
**Tip:** See ["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in this view's column headings

The **Open Key Incidents by Family** view lets you filter your view by the Family value. Possible Family values include:

- Address
- Aggregated Ports
- BGP
- Board
- Chassis
- Component Health
- Connection
- Correlation
- HSRP
- Interface
- License
- Node
- OSPF
- RAMS
- RMON
- RRP
- STP
- Trap Analysis

- VLAN
- VRRP

**Note:** By default, NNMi uses the first value in the Quick Filter list. If your view is empty, change the filter value. Here is an example of a Quick Filter list:



You can use this view to help you determine the types of incidents that are in the queue. For example, you might want to look at only incidents related to addresses or interfaces to help guide you in making troubleshooting decisions.

As with all incident views, you can filter this view by time period. The default time period is **Last Week** so that you can view all of the open incidents of a specified Family that have occurred within the last week.

**Note:** If you filter your view using multiple filters, NNMi uses the AND operator to combine the filters you have selected. See [Filter a Table View](#) for more information.

For each incident displayed, you can view its severity, its priority, its lifecycle state (for example **In Progress** or **Closed**), the date and time the incident last occurred, to whom the incident is assigned, the name of its source node, its source object, its category (for example, **Fault** or **Security**), its origin (for example, **Management Software** or **SNMP Trap**), the message used to describe the incident, and any related notes.

#### Related Topics

["Key Incident Views" \(on page 160\)](#)

["Organize Your Incidents" \(on page 133\)](#)

["Monitoring Incidents for Problems" \(on page 132\)](#)

["Display a Map from an Incident" \(on page 158\)](#)

["Key Incident Views" \(on page 160\)](#)

["Open Key Incidents View"](#)

["Unassigned Open Key Incidents View" \(on page 163\)](#)

["Open Key Incidents by Severity View" \(on page 164\)](#)

["Open Key Incidents by Priority View" \(on page 165\)](#)

["Open Key Incidents by Category View" \(on page 166\)"Open Key Incidents by Family View" \(on page 167\)](#)

["Closed Key Incidents View" \(on page 168\)](#)

["Key Incidents by Lifecycle State View" \(on page 169\)](#)

#### Closed Key Incidents View

**Tip:** See ["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in this view's column headings.

The **Closed Key Incidents** view displays the Key Incidents whose lifecycle state indicates that the incident has been closed. This view is useful for identifying the Key Incidents that have been resolved. This view might be particularly useful for reporting on how many incidents were closed within a given time period.



**Note:** Unlike other Key incident views, the Closed Key Incidents view includes incidents whose Correlation Nature is **Info**. The **Info** Correlation Nature is meant to be informational. Because Node Up incidents use this Correlation Nature, including incidents whose Correlation Nature is **Info** enables you to view any Node Down and Node Up incident pairs.

As with all incident views, you can filter this view by time period. The default time period is **Last Day** so that you can view all of the incidents whose Last Occurrence Time is within the last 24 hours. To select a more specific time range within a time period, you can filter the view using Last Occurrence Time values.

For each incident displayed, you can view its severity, the date and time the incident last occurred, to whom the incident is assigned, the name of its source node, its source object, its category (for example, **Fault** or **Security**), its family (for example, **Interface** or **Connection**), its origin (for example, **Management Software** or **SNMP Trap**), the message used to describe the incident, and any related notes.

See "[Monitoring Incidents for Problems](#)" (on page 132) for more information about ways to use incident views.

#### **Related Topics:**

[Use Table Views](#)

["Organize Your Incidents" \(on page 133\)](#)

["Monitoring Incidents for Problems" \(on page 132\)](#)

["Display a Map from an Incident" \(on page 158\)](#)

["Key Incident Views" \(on page 160\)](#)

["Open Key Incidents View" \(on page 161\)](#)

["Unassigned Open Key Incidents View" \(on page 163\)](#)

["Open Key Incidents by Severity View" \(on page 164\)](#)

["Open Key Incidents by Priority View" \(on page 165\)](#)

["Open Key Incidents by Category View" \(on page 166\)](#)

["Open Key Incidents by Family View" \(on page 167\)](#)

["Key Incidents by Lifecycle State View" \(on page 169\)](#)

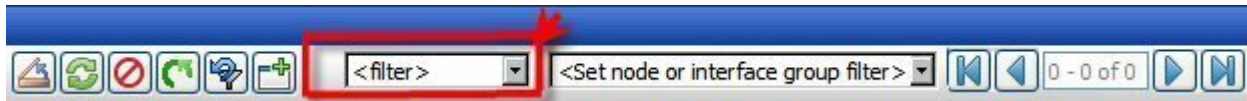
## **Key Incidents by Lifecycle State View**

**Tip:** See "[Incident Form](#)" (on page 134) for more details about the incident attributes that appear in this view's column headings

The **Key Incidents by Lifecycle State** view lets you filter your view by the Lifecycle State value. Possible Lifecycle State values include:

- Registered
- In Progress
- Completed
- Closed

**Note:** By default, NNMi uses the first value in the Quick Filter list. If your view is empty, change the filter value. Here is an example of a Quick Filter list:



Filter this view by the **Registered** Lifecycle State to view all new incidents. If your NNMi administrator set up Node Groups or Interface Groups to identify important elements of your environment, you can filter this view using the lifecycle state and Node Group filters. For example, you can display all of the incidents that are **In Progress** and are related to a certain group of nodes.

As with all incident views, you can filter this view by time period. The default time period is **Last Week** so that you can view all of the incidents of a specified lifecycle stat that have occurred within the last week.

**Note:** If you filter your view using multiple filters, NNMi uses the AND operator to combine the filters you have selected. See [Filter a Table View](#) for more information.

For each incident displayed, you can view its severity, its priority, the date and time the incident last occurred, to whom the incident is assigned, the name of its source node, its source object, its category (for example, **Fault** or **Security**), its family (for example, **Address** or **Connection**), its origin (for example, **Management Software** or **SNMP trap**), the message used to describe the incident, and any related notes.

#### Related Topics

["Key Incident Views" \(on page 160\)](#)

[Use Table Views](#)

["Organize Your Incidents" \(on page 133\)](#)

["Monitoring Incidents for Problems" \(on page 132\)](#)

["Display a Map from an Incident" \(on page 158\)](#)

["Key Incident Views" \(on page 160\)](#)

["Unassigned Open Key Incidents View" \(on page 163\)](#)

["Open Key Incidents View" \(on page 161\)](#)

["Open Key Incidents by Severity View" \(on page 164\)](#)

["Open Key Incidents by Priority View" \(on page 165\)](#)

["Open Key Incidents by Category View" \(on page 166\)](#)

["Open Key Incidents by Family View" \(on page 167\)](#)

["Closed Key Incidents View" \(on page 168\)](#)["Key Incidents by Lifecycle State View" \(on page 169\)](#)

#### Root Cause Incidents

**Tip:** See ["IP Address Form" \(on page 73\)](#)["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in a root cause incident view's column headings.

Root Cause Incidents identify the root cause, as well as symptoms associated with the root cause, as determined by NNMi's Causal Engine.

The Causal Engine uses ICMP and SNMP to constantly monitor your network. NNMi's Causal Engine uses the data collected from all the devices on your network to determine the root cause of known and potential problems. NNMi notifies you if it encounters any of the following situations:

- ["Node Down" \(on page 192\)](#)
- ["Node Down" \(on page 192\)](#)
- ["Interface Down" \(on page 188\)](#)
- ["Address Not Responding" \(on page 182\)](#)

NNMi provides the following Root Cause Incidents views:

- ["Root Cause Incidents View" \(on page 171\)](#)
- ["Open Root Cause Incidents View" \(on page 171\)](#)

**When using root cause incident views, note the following:**

- Your administrator may choose to configure particular incidents so that they appear as root cause incidents in your root cause views. To distinguish these incidents from those that NNMi itself identifies as root cause, the **Correlation Nature** value for incidents configured to be root cause by the NNMi administrator is **User Root Cause**.
- Any root cause view includes incidents that have a **Root Cause** value for **Correlation Nature**.
- Your administrator also determines whether to configure deduplication for particular incidents.

See ["Monitoring Incidents for Problems" \(on page 132\)](#) for more information about ways to use incident views.

**Related Topics:**

[Use Table Views](#)

["Organize Your Incidents" \(on page 133\)](#)

["Monitoring Incidents for Problems" \(on page 132\)](#)

["Display a Map from an Incident" \(on page 158\)](#)

## Root Cause Incidents View

**Tip:** See ["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in this view's column headings.

The Root Cause Incident view displays all of the root cause incidents. This view is useful for identifying the number of root cause incidents in the queue. You might then choose to narrow your focus by filtering this information according to one or more attribute values, such as all root cause incidents whose status is Critical, or all root cause incidents whose description is Node Down.

As with all incident views, you can filter this view by time period. The default time period is **Last Day** so that you can view all of the root cause incidents that have occurred within the last 24 hours.

For each incident displayed, you can view its severity, its priority, its lifecycle state (for example **In Progress** or **Closed**), the date and time the incident last occurred, to whom the incident is assigned, the name of its source node, its source object, its category (for example, **Fault** or **Security**), its family (for example, **Interface** or **Connection**), its origin (for example, **Management Software** or **SNMP Trap**), the message used to describe the incident, and any related notes.

See ["Monitoring Incidents for Problems" \(on page 132\)](#) for more information about ways to use incident views.

## Open Root Cause Incidents View

**Tip:** See "[Incident Form](#)" (on page 134) for more details about the incident attributes that appear in this view's column headings.

The **Open Root Cause Incidents** view displays the root cause incidents whose lifecycle state value indicates that the incident has not yet been closed. This view is useful for identifying the Root Cause Incidents that need to be resolved. As with all incident views, you can filter this view by time period. The default time period is **Last Week** so that you can view all of the Root Cause Incidents that have remained open within the last week.

For each incident displayed, you can view its severity, its priority, its lifecycle state (for example **In Progress** or **Closed**), the date and time the incident last occurred, to whom the incident is assigned, the name of its source node, its source object, its category (for example, **Fault** or **Security**), its family (for example, **Interface** or **Connection**), its origin (for example, **Management Software** or **SNMP Trap**), the message used to describe the incident, and any related notes.

You can also access additional views from this one using the Actions menu as described in [Use Table Views](#). One example of an action available from an open root cause incident view is the ability to access a map view of the nodes related to the incident.

### Related Topics:

[Use Table Views](#)

["Organize Your Incidents"](#) (on page 133)

["Monitoring Incidents for Problems"](#) (on page 132)

["Display a Map from an Incident"](#) (on page 158)

["Unassigned Open Key Incidents View"](#) (on page 163)

["Closed Key Incidents View"](#) (on page 168)

["Root Cause Incidents View"](#) (on page 171)

## Service Impact Incidents View

**Tip:** See "[Incident Form](#)" (on page 134) for more details about the incident attributes that appear in this view's column headings.

The **Service Impact Incidents** view displays all of the incidents whose Correlation Nature is **Service Impact**. Service Impact incidents indicate a relationship between incidents in which a network service is effected by other incidents. By default, NNMi generates Service Impact incidents for Router Redundancy Groups. For example, an Interface Down incident can effect a Router Redundancy Group that is part of an HSRP service. This view is useful for identify a service that is affected.

**Note:** The **Service Impact** Correlation Nature is available for use by NNM iSPi (HP Smart Plug-ins). See "Help for Administrators" for more information about HP Smart Plug-ins.

As with all incident views, you can filter this view by time period. The default time period is **Last Day** so that you can view all of the Service Impact incidents that have occurred within the last 24 hours.

For each incident displayed, you can view its severity, its priority, its lifecycle state (for example **In Progress** or **Closed**), the date and time the incident last occurred, to whom the incident is assigned, the name of its source node, its source object, its category (for example, **Fault** or **Security**), its family (for example, **Interface** or **Connection**), the message used to describe the incident, and any related notes.

See ["Monitoring Incidents for Problems" \(on page 132\)](#) for more information about ways to use incident views.

## Stream Correlation Incidents View

**Tip:** See ["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in this view's column headings.

The Stream Correlation Incidents view contains correlations that NNMi's event pipeline establishes as it recognizes patterns in the flow of events through the pipeline. Contact your NNMi administrator for more information about NNMi's event pipeline. Correlations are created as NNMi analyzes events and traps to determine the root cause incident for a problem. Examples of stream correlations include Dedup (duplication of events) and Rate (occurrence of events by time) correlations.

This view is useful for proactively identifying potential problems before they become critical or serious root cause incidents. Keeping these correlations in a separate view also reduces the number of root cause incidents in the queue.

As with all incident views, you can filter this view by time period. The default time period is **Last Week** so that you can view all of the correlations that have occurred within the last week.

For each correlation displayed, you can view its severity, its priority, its lifecycle state (for example **In Progress** or **Closed**), the date and time the correlation last occurred, to whom the correlation incident is assigned, the name of its source node, its source object, its category (for example, **Fault** or **Security**), its family (for example, **Interface** or **Connection**), the message used to describe the correlation incident, and any related notes.

See ["Monitoring Incidents for Problems" \(on page 132\)](#) for more information about ways to use incident views.

## Incidents by Family View

**Tip:** See ["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in this view's column headings.

The **Incidents by Family** view displays all of the incidents filtered by a specified Family; for example **Interface** or **Connection**. This view is useful for identifying the incidents of a particular type. As with all incident views, you can filter this view by time period. The default time period is **Last Day** so that you can view all of the incidents of a specified Family that have occurred within the last 24 hours.

For each incident displayed, you can view its severity, its priority, its lifecycle state (for example **In Progress** or **Closed**), the date and time the incident last occurred, to whom the incident is assigned, the name of its source node, its source object, its category (for example, **Fault** or **Security**), its origin (for example, **Management Software** or **SNMP Trap**), its Correlation Nature (for example, **Symptom** or **Root Cause**), the message used to describe the incident, and any related notes.

See ["Monitoring Incidents for Problems" \(on page 132\)](#) for more information about ways to use incident views.

## Custom Incidents View

**Tip:** See ["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in this view's column headings.

The **Custom Incidents** view lets you choose the columns of incident information, to better meet your needs. For example, you might want to filter the view to display only the incidents related to a particular set of devices. You might also want to filter the view to display only the incidents assigned to you.

This view includes most of the attributes available for the incident so that you can decide which are most important for you to display. See [Use Table Views](#) for more information about sorting, filtering, and hiding attributes within a view. As with all incident views, you can filter this view by time period. The default time period is **Last Day** so that you can view all of the incidents of interest that have occurred within the last 24 hours.

For each incident displayed, you can view its severity, its priority, its lifecycle state (for example **In Progress** or **Closed**), the date and time the incident last occurred, to whom the incident is assigned, the name of its source node, its source object, its category (for example, **Fault** or **Security**), its family (for example, **Interface** or **Connection**), its origin (for example, **Management Software** or **SNMP Trap**), its Correlation Nature (for example, **Symptom** or **Root Cause**), the message used to describe the incident, and any related notes. You can also view the duplicate count to indicate any duplicate occurrences of this incident, the name of the custom incident, an indicator of whether the NNMi root cause analysis (RCA) engine considers this incident to be active, any Correlation Notes that exist for the incident, the date and time the first instance of this incident occurred (if suppressing incidents), the date and time the original event that triggered the incident occurred, the date and time the incident was created, and the date and time the incident was last modified.

See [Filter a Table View](#) for more information about how to filter information displayed in a table.

See ["Monitoring Incidents for Problems" \(on page 132\)](#) for more information about ways to use incident views.

See ["Incident Form" \(on page 134\)](#) for more information about incident attributes.

#### **Related Topics:**

[Use Table Views](#)

["Organize Your Incidents" \(on page 133\)](#)

["Display a Map from an Incident" \(on page 158\)](#)

## **NNM 6.x/7.x Events View**

**Tip:** See ["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in this view's column headings.

The **NNM 6.x/7.x Events** view displays the incidents forwarded from Network Node Manager 6.x and 7.x management stations in your network environment.

You can use this view to monitor the health of devices being managed by previous versions of NNM, including NNM 6.x and NNM 7.x. You can also use this view to access the following 6.x/7.x features:

- **Actions** → **NNM 6.x/7.x Neighbor View**
- **Actions** → **NNM 6.x/7.x Details**
- **Actions** → **NNM 6.x/7.x ovw**

See ["Accessing NNM 6.x and 7.x Features" \(on page 209\)](#) for more information.

**Note:** You can only access 6.x/7.x features by selecting incidents generated from 6.x/7.x events.

For each incident displayed, you can view its severity, its lifecycle state (for example **In Progress** or **Closed**), the date and time the incident last occurred, the name of its source node, its category (for exam-

ple, **Fault** or **Security**), its family (for example, **Interface** or **Connection**), its Correlation Nature (for example, **Symptom** or **Root Cause**), the message used to describe the incident, and any related notes.

As with all incident views, you can filter this view by time period. The default time period is **Last Day** so that you can view all of the incidents of interest that have occurred within the last 24 hours.

## NNM 6.x/7.x Events by Category View

**Tip:** See ["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in this view's column headings.

The **NNM 6.x/7.x Events** by Category view displays the incidents forwarded from Network Node Manager 6.x and 7.x management stations in your network environment. This view enables you to filter the view by the Incident Category; for example **Fault**. As with all incident views, you can also filter this view by time period. The default time period is **Last Week** so that you can view all of the NNM 6.x or 7.x incidents that have occurred within the last week..

You can use this view to monitor the health of devices being managed by previous versions of NNM, including NNM 6.x and NNM 7.x.

For each incident displayed, you can view its severity, its lifecycle state (for example **In Progress** or **Closed**), the date and time the incident last occurred, the name of its source node, its family (for example, **Interface** or **Connection**), its Correlation Nature (for example, **Symptom** or **Root Cause**), the message used to describe the incident, and any related notes.

## SNMP Traps View

**Tip:** See ["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in this view's column headings.

The **SNMP Traps** view is useful for identifying all of the traps that were received from devices in your network environment. Your NNMi administrator must configure specific traps before they are displayed within NNMi incident views. As with all incident views, you can filter this view by time period. The default time period is **Last Hour** so that you can view all of the incidents of interest that have occurred within the last 24 hours.

For each incident displayed, you can view its severity, its lifecycle state (for example **In Progress** or **Closed**), the date and time the incident last occurred, the name of its source node, its source object, its category (for example, **Fault** or **Security**), its family (for example, **Interface** or **Connection**), its Correlation Nature (for example, **Symptom** or **Root Cause**), the message used to describe the incident, and any related notes.

## SNMP Traps by Family View

**Tip:** See ["Incident Form" \(on page 134\)](#) for more details about the incident attributes that appear in this view's column headings.

The **SNMP Traps by Family** view displays all of incidents whose source is an SNMP trap filtered by a specified Family; for example **Interface** or **Connection**. This view is useful for identifying the incidents of a particular type. As with all incident views, you can filter this view by time period. The default time period is **Last Day** so that you can view all of the incidents of a specified Family that have occurred within the last 24 hours.

For each incident displayed, you can view its severity, its priority, its lifecycle state (for example **In Progress** or **Closed**), the date and time the incident last occurred, the name of its source node, its source

or **Security**), its Correlation Nature (for example, **Symptom** or **Root Cause**), the message used to describe the incident, and any related notes.

See "[Monitoring Incidents for Problems](#)" (on page 132) for more information about ways to use incident views.



## Analyze Trap Information

By default, NNMi measures the rate of incoming SNMP traps, including the following:

- Traps from each device.
- Traps for each SNMP object identifier (OID).

NNMi monitors the incoming SNMP traffic flow to determine whether the number of traps received within a certain time period exceeds any set threshold. If a threshold is exceeded, NNMi blocks receipt of additional traps until the number of traps falls below the threshold set for each time period.

**Note:** The NNMi administrator can configure threshold values using the `nnmtrapconfig.ovpl` script.

(*NNM iSPI Network Engineering Toolset*) If NNM iSPI NET is available in your network environment, you can obtain reports about incoming SNMP traps according to the following criteria:

- Within a specific time period
- For a specific node
- For a specific SNMP trap identifier (trap OID)

For more information about NNM iSPI NET, [click here](#).

When analyzing traps, NNMi looks at both the most common traps as well as the most common source nodes from which the traps are received. NNMi logs this SNMP trap analytics data to the `trap-analytics.0.0.log` file. NNMi organizes the information in the log file according to the following criteria:

- Trap rate in number of traps per second
- The top 10 addresses that are generating traps
- The top 10 traps that are being generated

To make this data more easily available, use the `nnmtrapdump.ovpl` command. This NNM iSPI NET tool enables you to extract the data in which you are most interested from the `trapanalytics.0.0.log` file.

See the [nnmtrapdump.ovpl](#) Reference Page for more information (**Help** → **Documentation Library** → **Reference Pages**, in the *User Commands* category).

## Investigate and Diagnose Problems

NNMi offers several ways for you to investigate and diagnose network problems.

- Use the Actions menu to gather the latest information about multiple aspects of a node (rather than waiting for the next regularly scheduled collection time).
  - ["Verify Device Configuration Details " \(on page 177\)](#)
  - ["View the Monitoring Configuration Details" \(on page 178\)](#)
  - ["Verify Current Status of a Device" \(on page 180\)](#)
- The Causal Engine keeps track of changes in your network, and alerts you to the root cause of problems and potential problems. See ["Interpret Root Cause Incidents" \(on page 181\)](#) for more information.
- The Actions menu also provides an easy way to launch troubleshooting commands to diagnose node connectivity and access problems:
  - ["Display End Nodes Attached to a Switch" \(on page 204\)](#)
  - ["Test Node Access \(Ping\)" \(on page 206\)](#)
  - ["Find the Route \(traceroute\)" \(on page 206\)](#)
  - ["Establish Contact with a Node \(telnet\)" \(on page 207\)](#)
  - ["Check Status Details for a Node Group" \(on page 208\)](#)
  - ["Accessing NNM 6.x and 7.x Features" \(on page 209\)](#)
- Use the Tools menu to find a problem node. You can also use the Tools menu to verify that NNMi, itself, is running properly. This includes checking the status of NNMi processes and services:
  - ["Find a Node" \(on page 203\)](#)
  - ["Find the Attached Switch Port" \(on page 204\)](#)
  - ["Checking the Status of NNMi" \(on page 211\)](#)

## Verify Device Configuration Details

Before you begin diagnosing a problem, you might want to gather current information about a node to update information in views and NNMi maps.

**Note:** NNMi automatically gathers this information according to the Rediscovery Interval setting that was set by your administrator. The minimum allowed Rediscovery Interval setting is 1 hour. The default value set by NNMi is 24 hours.

### To update your discovery information for a node:

1. Navigate to the view or form of interest and select the node whose discovery information you want to update.

#### To navigate to a table view and select a node



- a. From the workspace navigation panel, select the workspace of interest; for example, **Inventory**.
- b. Click the view that contains the node whose communication settings you want to check; for example **Nodes**.

- c. From the table view, click the  selection box that precedes the node whose configuration you want to check.

**To navigate to a map view and select a node:**

- a. Navigate to the table view.
- b. From a table view, click the  selection box that precedes the node of interest.
- c. Select **Actions**.
- d. From the drop-down menu, select the map view of interest.
- e. From the map view, click the node whose configuration you want to check.

**To select a node from a form:**

- a. From a table view, click the  Open icon that precedes the node of interest.
- b. From a map view, click the node of interest on the map and click the  Open icon.

2. Select **Actions** → **Configuration Poll**.

As the node is polled, NNMi displays the status messages for the Layer 3 discovery information. A Layer 2 connectivity analysis is also started. Information collected includes the node's IP address, subnet, contact name, location, and description.

## View the Monitoring Configuration Details

Use the **Actions** → **Monitoring Settings** menu item to display the current monitoring configuration settings for a particular node, interface, address, Router Redundancy Member, Tracked Object, or Node Component.

NNMi can be configured to monitor several aspects of each device, and provide a wealth of information to help you do your job. After fault polling is enabled, several NNMi processes work together to detect problems and quickly calculate the device status and the root cause of any problems for you.

*(NNM iSPI Performance for Metrics)* The NNM iSPI Performance for Metrics software can monitor performance statistics and thresholds for each interface.

### Monitoring Possibilities

Attribute	Description
Node Group	The name of any Node Groups to which this device belongs. See <a href="#">About Node and Interface Groups</a> for more information.
Fault Polling (SNMP and ICMP)	<p>If enabled, State Poller monitors all managed interfaces, IP addresses, and SNMP agents by issuing ICMP pings and SNMP read-only queries for MIB II ifAdminStatus and ifOperStatus. (ifAdminStatus is set by the device administrator. ifOperStatus indicates the overall health of the device and is supplied by the SNMP Agent.)</p> <p>If disabled:</p> <ul style="list-style-type: none"> <li>• Devices that were already discovered remain with the last calculated state/status.</li> <li>• Newly discovered devices are set to "No Status" with map-symbol background shape color set to beige.</li> </ul>



Attribute	Description
Fault Polling Interval	The time that State Poller waits between issuing queries to gather information.
Performance Polling	<p>(<i>NNM iSPI Performance for Metrics</i>)</p> <p>If enabled, the NNM iSPI Performance for Metrics software is installed. The the NNM iSPI Performance for Metrics software is accessed from the Action menu within map views and table views.</p> <p>If disabled, network performance data is not currently available.</p>
Performance Polling Interval	<p>(<i>NNM iSPI Performance for Metrics</i>)</p> <p>The time that the NNM iSPI Performance for Metrics software waits between issuing queries to gather information.</p>

**To view the monitoring configuration for a Node, Interface, or IP address:**



1. Navigate to the view for that object (for example, **Inventory** workspace, **Nodes** view).
2. Select the object of interest by selecting the  check box that precedes the object information.
3. Select **Actions** → **Monitoring Settings**.

**Note:** This menu item also is available on any object's form.


**To view the monitoring configuration for a Router Redundancy Member:**

1. Navigate to a Router Redundancy Group view (for example, **Inventory** workspace, **Router Redundancy Groups** view).
2. Click the  Open icon that precedes the Router Redundancy Group of interest.
3. From the Router Redundancy Members tab, click the  Open icon that precedes the Router Redundancy Group Member of interest.
4. Select **Actions** → **Monitoring Settings**.

**To view the monitoring configuration for a Tracked Object:**

1. Navigate to a Router Redundancy Group view (for example, **Inventory** workspace, **Router Redundancy Groups** view).
2. Click the  Open icon that precedes the Router Redundancy Group of interest.
3. From the Router Redundancy Members tab, click the  Open icon that precedes the Router Redundancy Group Member of interest.
4. Select the Tracked Object of interest by selecting the  check box that precedes the object information.
5. Select **Actions** → **Monitoring Settings**.

**To view the monitoring configuration for a Node Component:**

1. Navigate to a Node view (for example, **Inventory** workspace, **Nodes** view).
2. Click the  Open icon that precedes the Node of interest.
3. Select the **Component Health** tab.

4. Select the Node Component of interest by selecting the  check box that precedes the object information.
5. Select **Actions** → **Monitoring Settings**.

**Note:** This menu item is also available on any **Node Component** form.

## Verify Current Status of a Device

NNMi calculates the status of devices each time additional information is gathered from various sources. You can instruct NNMi to gather real-time data for all the information that NNMi uses to calculate Status for each selected Node or selected Incident's Source Node (up to maximum 10).

### To update node status information:

1. Navigate to the view of interest and select each node whose status information you want to update. Do one of the following:

#### Navigate to a table view and select up to 10 nodes:

- a. From the workspace navigation panel, select the workspace of interest; for example, **Inventory**.
- b. Click the view that contains the nodes whose status you want to update; for example **Nodes**.
- c. From the table view, click the  selection box that precedes each node whose status you want to update (maximum 10).

#### Navigate to a map view and select up to 10 nodes:

- a. Navigate to the **Topology Maps** workspace.
- b. Open the map view.
- c. Click or Ctrl-click each node whose status you want to update (maximum 10).

#### Navigate to an incident view and select up to 10 incidents:

- a. Navigate to the **Incident Management** or **Incident Browsing** workspace.
- b. From a table view, click the  selection box that precedes each incident whose Source Node status you want to update (maximum 10).

2. Select **Actions** → **Status Poll**.
3. A window for each Node displays with a report about which information was gathered. Your NNMi administrator determines the list of information gathered by establishing Monitoring Configuration settings.

### Status Poll Data Returned

Item	Description
Policy	Describes the item being gathered.
Target	Identifies where the information is being gathered.
Poller	The name of the Polling Policy that NNMi State Poller uses to control what is gathered. The following additional information is displayed: <ul style="list-style-type: none"><li>■ Whether or not the target is responding.</li><li>■ Whether or not the poll was successful.</li></ul>

Item	Description
	<ul style="list-style-type: none"><li>How long it took to get an answer.</li></ul>
Resulting Data	Shows the results for this item.









**To see the resulting Node status after the real-time update:**

Do one of the following:

- Open the appropriate Node form, see ["Accessing Device Details" \(on page 27\)](#). Check the information displayed on the ["Node Form: Status Tab" \(on page 48\)](#) and the ["Node Form: Component Health Tab" \(on page 40\)](#).
- Check the Node icon status colors on maps (["Watch Status Colors" \(on page 129\)](#)).
- In a Node view, locate the row representing the node and check the icon in the Status column.
- From the Incident form, launch the Source Node's form, see ["Incident Form" \(on page 134\)](#) for instructions about using the Source Node attribute to launch the appropriate Node form.

## Interpret Root Cause Incidents

The Causal Engine keeps track of changes in your network, and alerts you to the root cause of problems and potential problems. The Causal Engine sets an object's status using an object's outstanding conclusions. Every outstanding conclusion has a status, such as **Normal** or **Critical**. The highest status for an object's outstanding conclusions becomes the object's status. The order of status from lowest to highest is listed below:

-  No Status
-  Normal
-  Disabled
-  Unknown
-  Warning
-  Minor
-  Major
-  Critical

**Incident views** explain the situation. Click here for examples of the type of information you can obtain from incidents. The information in the Incident helps you solve the problem quickly and efficiently:

- A router, switch, server, or other monitored device is down (see ["Node Down" \(on page 192\)](#))
- A node or connection might be down and need your attention (see ["Node or Connection Down" \(on page 194\)](#))
- An interface is operationally down (see ["Interface Down" \(on page 188\)](#))
- An address is no longer responding (see ["Address Not Responding" \(on page 182\)](#)).

- The connection between two important devices is down (see ["Connection Down" \(on page 186\)](#) and ["Connection Partially Unresponsive" \(on page 187\)](#))

**Map views** provide a quick way to view status. Click here for more information. As problems are detected for specific devices, the Causal Engine changes the status color of that device's icon on the maps. See ["Watch Status Colors" \(on page 129\)](#) for more information about status color.

The sequence of color changes indicates increasing levels of trouble. Red, the most severe, indicates that a network element is not functioning. You generally want to intervene and solve problems before they cause a complete node failure.

For more information about root cause scenarios, see the following:

- ["Node Down" \(on page 192\)](#)
- ["Address Not Responding" \(on page 182\)](#)
- ["Address Disabled" \(on page 182\)](#)
- ["Interface Down" \(on page 188\)](#)
- ["Interface Disabled" \(on page 189\)](#)
- ["Interface Unmanageable" \(on page 190\)](#)
- ["Connection Down" \(on page 186\)](#)
- ["Connection Partially Unresponsive" \(on page 187\)](#)
- ["Node or Connection Down" \(on page 194\)](#)
- ["SNMP Agent Not Responding" \(on page 196\)](#)
- ["Non-SNMP Node Unresponsive" \(on page 195\)](#)

## Address Disabled

NNMi generates an **Address Disabled** conclusion when its interface becomes disabled. (An interface is disabled when its Administrative State (MIB II ifAdminStatus) is set to **Down**. See ["Interface Disabled" \(on page 189\)](#) for more information.)

**Note:** When the Administrative State is set to **Down**, the State of the address is set to **Not Responding**. If the interface's Administrative State changes to **Up**, but the Operational State remains **Down**, the address State remains set to **Not Responding**.

In the **Conclusions** list, trouble with an address is indicated by the following:

```
AddressesDisabled
```

An **Address Disabled** conclusion does not generate an incident, but appears in the information that is accessible from the Conclusions tab in the IP Address form.

## Address Not Responding

NNMi periodically uses an ICMP ping command to check each address. If there is no response, NNMi's Causal Engine determines that the address is not responding:

On the source Node form, NNMi updates information on the following tabs:

- **Addresses**
- **Interfaces**

- **Status**
- **Conclusions**
- **Incidents**

In the **Conclusions** list, trouble with an address is indicated by the following:

`SomeUnresponsiveAddressesInNode (node status = Minor)`

**Note:** If you view an `AllUnresponsiveAddressesInNode` conclusion, see ["Node Down" \(on page 192\)](#) for more information.

On the maps, the icon for the Node is set to yellow (status = Minor), and any Interfaces that are using this address are updated.

**Note:** If the interface has more than one address, the address symbol might stay green (status = normal):



## **Aggregator Interface Degraded (NNMi Advanced)**

NNMi generates an Aggregator Interface Degraded incident when the Status of at least one of the physical interfaces that is a member of an Aggregator Interface is set to **Critical**. See [Layer 2 Neighbor View Map Objects](#) for more information about Aggregator Interfaces.

An Aggregator Interface Degraded incident has a Severity set to **Minor**.

**On the Incident form**, Information on the following tabs is updated:

- Correlated Parents
- Correlated Children

**Note:** When an Interface Up occurs for all of the physical interfaces whose Status is **Critical**, NNMi updates Information in the **Correlation Notes** attribute and closes the incident.

**On the Interface form for the Aggregator Interface**, the Interface **State** attributes are updated. Information on the following tabs is updated:

- Addresses (if the interface has one or more addresses)
- Status
- Conclusions
- Incidents

In the **Conclusions** list, trouble with each physical interface that is a member of the Aggregator Interface is indicated by the following:

`InterfaceDown (Interface status = Critical)`

See ["Interface Down" \(on page 188\)](#) for more information about Interface Down incidents.

**On Layer 2 Neighbor View maps**, the icon for the Aggregator Interface is yellow:





When an Interface Up occurs for all of the physical interfaces whose Status is **Critical**, NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "[Incident Form: General Tab](#)" (on [page 135](#)) for more information.

## Aggregator Interface Down (NNMi Advanced)

NNMi generates an Aggregator Interface Down when the Status of all physical interfaces that are members of the Aggregator Interface are set to **Critical**.

An Aggregator Interface may become Critical when NNMi determines either of the following:

- The Aggregator Interface exists in the interface table and its MIB II ifOperStatus is Down.
- All of the physical interfaces that are members of the Aggregator Interface have a MIB II ifOperStatus of Down.

See [Layer 2 Neighbor View Map Objects](#) for more information about Aggregator Interfaces.

An Aggregator Interface Down incident has Severity set to **Critical**

**On the Incident form**, Information on the following tabs is updated:

- Correlated Parents
- Correlated Children

**Note:** When an Interface Up occurs for any of the physical interfaces, NNMi updates Information in the **Correlation Notes** attribute and closes the incident.

**On the Interface form for the Aggregator Interface**, the Interface **State** attributes are updated. Information on the following tabs is updated:

- Addresses (if the interface has one or more addresses)
- Status
- Conclusions
- Incidents

In the **Conclusions** list, trouble with each physical interface that is a member of the Aggregator Interface is indicated by the following:

InterfaceDown (Interface status = Critical)

See "[Interface Down](#)" (on [page 188](#)) for more information about Interface Down incidents.

**On Layer 2 Neighbor View maps**, the icon for the Aggregator Interface is red:



When an Interface Up occurs for any of the physical interfaces, NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "[Incident Form: General Tab](#)" (on [page 135](#)) for more information.

## Aggregator Connection Degraded (NNMi Advanced)

NNMi generates an Aggregator Connection Degraded incident when the Status of at least one of the Aggregator Interfaces that is a member of a Link Aggregation is set to **Minor**. See [Layer 2 Neighbor View Map Objects](#) for more information about Aggregator Connections. Also see ["Aggregator Interface Degraded \(NNMi Advanced\)" \(on page 183\)](#).

An Aggregator Connection Degraded incident has a Severity set to **Minor**.

**On the Incidents form**, Information on the following tabs is updated:

- Correlated Parents
- Correlated Children

**Note:** When an Interface Up occurs for all of the physical interfaces whose Status is **Critical**, NNMi updates Information in the **Correlation Notes** attribute and closes the incident.

**On the Layer 2 Connection form for the Aggregator Connection**, the Interface **State** attributes are updated. Information on the following tabs is updated:

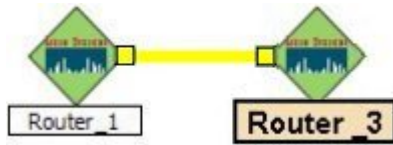
- Status
- Conclusions
- Incidents

In the **Conclusions** list, trouble with each physical interface that is a member of the Link Aggregation is indicated by the following:

InterfaceDown (Interface status = Critical)

See ["Interface Down" \(on page 188\)](#) for more information about Interface Down incidents.

**On Layer 2 Neighbor View maps**, the thick line for the Aggregator Connection is yellow:



When an Interface Up occurs for all of the physical interfaces whose Status is **Critical**, NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See ["Incident Form: General Tab" \(on page 135\)](#) for more information.

## Aggregator Connection Down (NNMi Advanced)

NNMi generates an Aggregator Connection Down incident when the Status of at least one of the Aggregator Interfaces that is a member of the Link Aggregation is set to **Critical**. See [Layer 2 Neighbor View Map Objects](#) for more information about Aggregator Interfaces and Aggregator Connections. Also see ["Aggregator Interface Down \(NNMi Advanced\)" \(on page 184\)](#).

An Aggregator Connection Down incident has Severity set to **Critical**.

**On the Incident form**, Information on the following tabs is updated:

- Correlated Parents
- Correlated Children

**Note:** When an Interface Up occurs for any of the physical interfaces, NNMi updates Information in the **Correlation Notes** attribute and closes the incident.

**On the Layer 2 Connection form for the Aggregator Connection**, the Interface **State** attributes are updated. Information on the following tabs is updated:

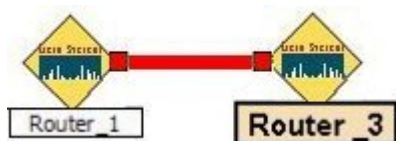
- Status
- Conclusions
- Incidents

In the **Conclusions** list, trouble with each physical interface that is a member of the Link Aggregation is indicated by the following:

InterfaceDown (Interface status = Critical)

See "[Interface Down](#)" (on page 188) for more information about Interface Down incidents.

**On Layer 2 Neighbor View maps**, the thick line indicating the Aggregator Connection is red:



When an Aggregator Connection Up occurs, NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "[Incident Form: General Tab](#)" (on page 135) for more information.

## Buffer has Insufficient Capacity or is Malfunctioning

A **Buffer has Insufficient Capacity or is Malfunctioning** incident indicates the buffer pool for the source node is either exhausted or cannot meet the demand for use.

A **Buffer has Insufficient Capacity or is Malfunctioning** incident is generated with Severity set to **Critical**.

On the Source Node form, information on the following tabs is updated:

- **Correlated Children**
- **Status**
- **Conclusions**

The Correlated Children tab includes any associated traps.

On the map, the Causal Engine sets the color of the Source Node to yellow.

## Connection Down

NNMi periodically uses SNMP to check the interface on each end of a connection. NNMi's Causal Engine uses this information to determine the status of the connection. If both ends of the connection are down, the Causal Engine determines that the connection is down.

A **Connection Down** incident is generated with Severity set to **Critical**. The information on the following tab is updated:

- **Correlated Children**

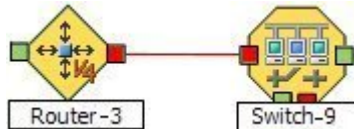
On the **Connections** form, information on the following tabs is updated:






- **Interfaces**
- **Status**
- **Conclusions**

In the **Conclusions** list, trouble with a connection is indicated by the following:

- `ConnectionDown` (connection status = Critical)

On the maps, the Causal Engine sets the color of the line between the devices according to the following criteria (the line indicates the connection):



-  Red: neither interface is responding.
-  Green: Both interfaces are responding.
-  Yellow: the interface on one end is not responding. The interface on the other end is responding.
-  Light Blue: due to other network problems, the status of one interface cannot be determined at this time.
-  Dark Blue: due to other network problems, the status of both interfaces cannot be determined at this time.

## Connection Partially Unresponsive

NNMi periodically uses SNMP to check the interface on each end of a connection. NNMi's Causal Engine uses this information to determine the status of the connection. If NNMi cannot determine the status of one end of a connection and the other end of the connection is up, the Causal Engine determines that the connection is partially unresponsive. In the case of multiple end points within a connection, at least one end point must be up. The remaining end points must be a combination of up and unresponsive (meaning NNMi cannot determine the status of the end point).

Reasons NNMi might not be able to determine the status of an interface is that a problem exists in an ATM or FrameRelay cloud that is between one interface and the other.

A **Connection Partially Unresponsive** incident is generated with Severity set to **Critical**.

On the **Connections** form, information on the following tabs is updated:

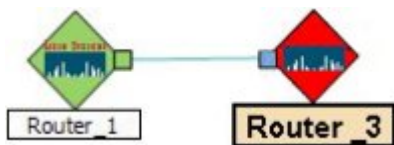
- **Interfaces**
- **Status**
- **Conclusions**

In the **Conclusions** list, trouble with a connection is indicated by the following:

- `ConnectionPartiallyUnresponsive` (connection status =Warning)

If the source node is in the Important Nodes Group, the Node Down incident appears as a correlated child under the Connection Partially Unresponsive incident. (Your administrator decides what nodes belong in the Important Nodes group.)

On the maps, the Causal Engine sets the color of the line between the devices as follows (the line indicates the connection):



## CPU Utilization is too High

A **CPU Utilization is too High** incident indicates any of the following utilization averages is too high:

- 5 second
- 1 minute
- 5 minute

A **CPU Utilization is too High** incident is generated with Severity set to **Critical**.

On the Source Node form, information on the following tabs is updated:

- **Correlated Children**
- **Status**
- **Conclusions**

The Correlated Children tab includes any associated traps.

On the map, the Causal Engine sets the color of the Source Node to yellow.

## Fan is Malfunctioning

A **Fan is Malfunctioning** incident indicates the identified fan on the Source Node is not operating correctly.

A **Fan is Malfunctioning** incident is generated with Severity set to **Critical**.

On the Source Node form, information on the following tabs is updated:

- **Correlated Children**
- **Status**
- **Conclusions**

The Correlated Children tab includes any associated traps.

On the map, the Causal Engine sets the color of the Source Node to yellow.

## Interface Down

NNMi periodically uses SNMP to check each interface. If an SNMP agent reports that an interface is down (MIB II ifOperStatus), NNMi's Causal Engine takes the following actions:

An Interface Down incident is generated with Severity set to **Critical**. Information on the following tabs is updated:

- Correlated Parents
- Correlated Children
- Custom Attributes

Information in the **Correlation Notes** attribute is updated on an Interface Up.

**Note:** You might find relevant traps as Correlated Children on the Correlations tab.

On the **Interface** form, the **Interface State** attributes are updated. Information on the following tabs is updated:

- Addresses (if the interface has one or more addresses)
- Status
- Conclusions
- Incidents

In the **Conclusions** list, trouble with an interface is indicated by the following:

`InterfaceDown` (Interface status = Critical)

On the source Node's form, the information on the following tabs is updated:

- Addresses
- Interfaces
- Status
- Conclusions
- Incidents

In the **Conclusions** list, trouble with an interfaces is indicated by the following:

`InterfacesDownInNode` (node status = Minor)

On the maps, the icons for the node and its interfaces are updated:



When an Interface Up occurs, NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See ["Incident Form: General Tab" \(on page 135\)](#) for more information.

## Interface Disabled

NNMi periodically uses SNMP to check each interface. If an SNMP agent reports that an interface is administratively down (MIB II ifAdminStatus), NNMi's Causal Engine takes the following actions:

**Note:** Interface Disabled incidents are not generated by default. Your NNMi administrator must configure these incidents to be generated.

An Interface Disabled incident is generated with Severity set to **Critical**. Information on the following tabs is updated:

- Correlated Children
- Custom Attributes

Information in the **Correlation Notes** attribute is updated on an Interface Enabled.

**Note:** You might find relevant traps on the **Correlations** tab.

On the **Interface** form, the **Interface State** attributes are updated. Information on the following tabs is updated:

- Addresses
- Status
- Conclusions
- Incidents

In the **Conclusions** list, trouble with an interface is indicated by the following:

InterfaceDisabled (Interface status = **Disabled**)

On the source Node's form, the information on the following tabs is updated:

- Addresses
- Interfaces
- Status
- Conclusions
- Incidents

On the maps, the icons for any of the node's disabled interfaces are updated and displayed as grey (disabled):



When an Interface Enabled occurs, NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See ["Incident Form: General Tab" \(on page 135\)](#) for more information.

## Interface Unmanageable

NNMi periodically uses SNMP to check each interface. If an SNMP agent is not responding, NNMi's Causal Engine takes the following actions:

One `InterfaceUnmanageable` message is generated for each interface within the node.

On each **Interface** form, the **Interface State** attributes are updated. The information on the following tabs is updated:

- Addresses
- Status
- Conclusions

In the **Conclusions** list, trouble with the interface is indicated by the following:

InterfaceUnmanageable (Interface status = Unknown)

On the source node's form, the **SNMP Agent State** attributes are updated. The information on the following tabs is updated:

- Addresses (if the interface has one or more IP addresses)
- Interface
- Status
- Conclusions
- Incidents

In the **Conclusions** list, trouble with an interface is indicated by the following:

UnresponsiveAgentInNode (status = Minor)

**Note:** There is one `InterfaceUnmanageable` message for each interface within the node.

On the maps, the icons for the node and its interfaces are updated:

If the interface is unmanageable because the SNMP agent is down:



If the interface is unmanageable because of a node down situation:



## Remote Site Containing Node <Source Node Name> is Unreachable

A Remote Site is Unreachable incident is generated when all of the nodes in an Island Node Group do not respond to ICMP or SNMP queries.

An Island Node Group is a group of connected nodes that NNMi discovers and that are not connected to the rest of the topology. An example of an environment with multiple Island Node Groups is a financial institution or retail store with many branches or stores. Each branch or store might be connected to other branches or stores with a WAN (Wide Area Network) connection. Each branch or store appears as an isolated island of nodes in the NNMi topology.

NNMi automatically creates Island Node Groups whenever it detects changes in Layer 2 connections.

NNMi selects a representative node in each Island Node Group as the Source Node associated with the Remote Site incident. The Source Object is the Island Node Group.

## Memory has Insufficient Capacity or is Malfunctioning

A **Memory has Insufficient Capacity or is Malfunctioning** incident indicates the memory pool for the Source Node is exhausted or cannot meet the demand for use.



A **Memory has Insufficient Capacity or is Malfunctioning** incident is generated with Severity set to **Critical**.

On the Source Node form, information on the following tabs is updated:

- **Correlated Children**
- **Status**
- **Conclusions**

The Correlated Children tab includes any associated traps.

On the map, the Causal Engine sets the color of the Source Node to yellow.

## Node Down

An unresponsive device within your network can cause a variety of problems. If the troubled device is a router, switch, or server, many devices could be unreachable. You receive a Node Down incident when NNMi analyzed the situation and determined any of the following:

- [A node with two or more connections is truly down.](#)
- [An SNMP node that has no discovered connections is unreachable.](#)
- [A node belongs to the Important Nodes Group and has become unreachable.](#) Your NNMi administrator assigns devices to this Node Group (these devices can have any number of connections).
- [A non-SNMP node is unreachable.](#)

A Node Down incident is generated with Severity set to **Critical**, and the map icon is set to red (see [Map Displays](#)). Any Interface Down incident on neighbors that are one hop from the node are correlated under the Node Down incident.

**Note:** When NNMi cannot determine whether the node or connection is down, it generates a **Node or Connection Down** incident. See "[Node or Connection Down](#)" (on page 194) for more information.

NNMi does not generate a Node Down incident under the following conditions:

- If the node is in the shadow of another problem that causes the to be unreachable.
- If the node is in an ATM or FrameRelay cloud that causes the node to be unreachable.

### When the Node Has Two or More Connections

The Causal Engine uses the following criteria to verify which node is actually down:

**Note:** If the addresses are not being polled, only the last two criteria are used.

Stand-Alone Problem	Side Effect of Another Problem	Criteria
+	+	100% of the addresses assigned to this node are unreachable.
+	+	The SNMP agent installed on this machine is not responding.
+	-	At least two of the neighboring devices can be reached and are reporting problems with connectivity to this node. Therefore, this is not a "Shadow" problem, but is truly a problem with the identified node.

In the device's Node form, the Conclusions tab shows the relevant combination of conclusions, which might include any of the following:

- `AllUnresponsiveAddressesInNode` (status = Minor) - (Appears only when addresses are being polled)
- `UnresponsiveAgentInNode` (status = Minor)
- `NodeWithAtleastTwoNeighborsUp` (status = Normal)

#### **When the SNMP Node has No Discovered Connections and is Unreachable**

The Causal Engine generates a Node Down incident for an SNMP node when an unconnected node is unreachable. (No connections have been discovered for the node.)

#### **When a Node is in the Important Nodes Group**

When a Node in the Important Node Group is unreachable, NNMi issues a Node Down incident.

Nodes in the Important Nodes Group may or may not have two or more connections. See ["Connection Partially Unresponsive" \(on page 187\)](#) for more information about how nodes in an Important Node Group are handled when the connection is partially unresponsive.

#### **When a non-SNMP Node is Unreachable**

The Causal Engine generates a Node Down incident for a non-SNMP node under the following conditions:

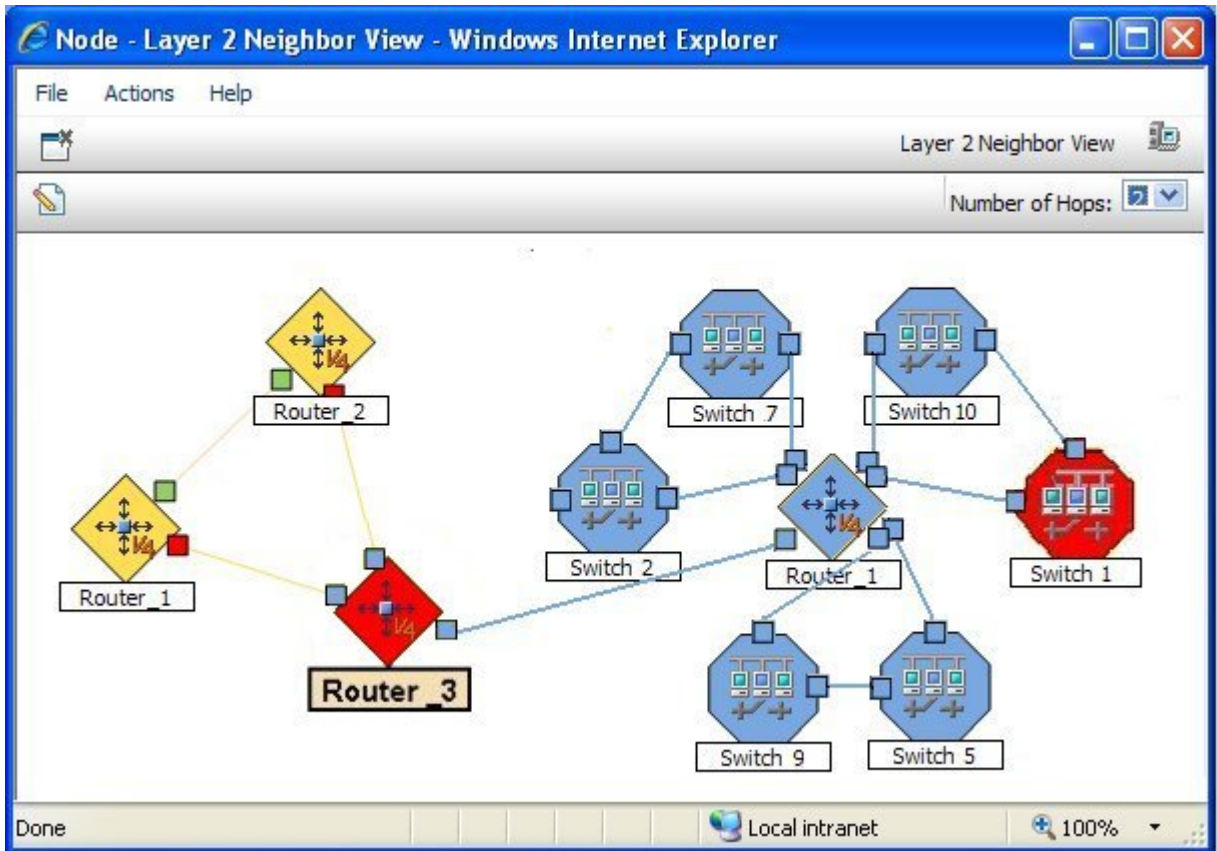
- The interface on an SNMP node at one end of a connection is Down.
- The non-SNMP end node on the other end of the connection does not respond to ping.

#### **Map Displays**

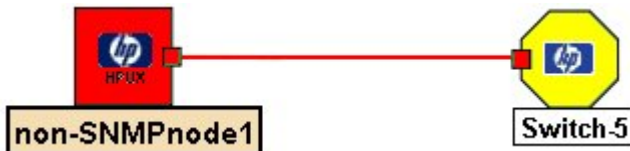
The Status of the Node Down device for an SNMP node changes to **Critical** and the device's map icon color changes to red (Router 3 in the illustration below). The status of each unreachable interface changes to **Unknown** and the interface map icon color changes to blue.

Any other devices that are unreachable *because of this problem* are in the "shadow" of the problem:

- The unreachable shadow devices' map icons change to blue.
- Members of the Important Nodes group's map icons change to red (Switch 1 in the illustration below).



The Status of the Node Down device for a non-SNMP node changes to **Critical** and the device's map icon color changes to red. The Status of the interface on each end of the connection also changes to **Critical** and each interface's map icon color changes to red.



When a Node Up occurs, NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "[Incident Form: General Tab](#)" (on page 135) for more information.

## Node or Connection Down

If a node is not responding to ICMP and SNMP queries, and only one neighbor is down, the Causal Engine cannot determine whether the node itself is down or whether the connection to the node is down.

A Node or Connection Down incident is generated with Severity set to **Critical**.

On the source node's form, the information on the following tabs is updated:

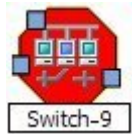
- Addresses
- Interface
- Status

- Conclusions
- Incidents

In the **Conclusions** list, trouble is indicated by the following message:

`NodeOrConnectionDown (node status = Critical)`

On the maps, the icon for the node is set to red:



## Non-SNMP Node Unresponsive

NNMi generates a **Non-SNMP Node Unresponsive** incident under the following conditions:

- A node does not have an SNMP agent
- NNMi is unable to ping all of the addresses for the non-SNMP node

Reasons NNMi might not be able to ping all of the addresses for a node include one or more devices between the non-SNMP node and its neighbor device are down.

**Note:** If a node does not have an SNMP agent, NNMi is able to gather only the address information for the node.

A **Non-SNMP Node Unresponsive** incident is generated with Severity set to **Critical**.

On the node form, information on the following tabs is updated:

- **Status**
- **Conclusions**

In the **Conclusions** list, trouble with a connection is indicated by the following:

- `Non-SNMPNodeUnresponsive (node status =Critical)`

On the maps, NNMi's Causal Engine sets the color of the node to red:



## Number of SNMP Traps Persisted in the Database has Reached or Exceeded Trap Limit

A **Number of SNMP Traps Persisted in the Database has Reached or Exceeded Trap Limit** incident indicates the number of SNMP traps has reached or exceeded the maximum limit. By default, the SNMP trap limit is 100,000.

**Note:** When the maximum limit is reached, NNMi no longer accepts traps from the Event system. The NNMi administrator can reduce the number of traps in the NNMi database. See the `nnmtri-mincidents.ovpl` Reference Page (**Help** → **Documentation Library** → **Reference Pages**, in the *Administrator Commands* category).

A **Number of SNMP Traps Persisted in the Database has Reached or Exceeded Trap Limit** incident is generated with Severity set to **Critical**.

## Power Supply is Malfunctioning

A **Power Supply is Malfunctioning** incident indicates the Source Node's specified power supply is not operating correctly.

A **Power Supply is Malfunctioning** incident is generated with Severity set to **Critical**.

On the Source Node form, information on the following tabs is updated:

- **Correlated Children**
- **Status**
- **Conclusions**

The Correlated Children tab includes any associated traps.

On the map, the Causal Engine sets the color of the Source Node to yellow.

## SNMP Agent Not Responding

NNMi periodically uses SNMP to check the availability of each SNMP Agent in your network environment. If an SNMP Agent is not responding (for example, the SNMPv1 or SNMPv2c community string for this agent changed, or the SNMPv3 user name for this agent changed, and the NNMi communication configuration settings have not yet been updated):

On the source node's form, the **SNMP Agent State** attributes are updated. The information on the following tabs is updated:

- Interface
- Status
- Conclusions

In the **Conclusions** list, trouble with an SNMP agent is indicated by the following:

`UnresponsiveAgentInNode` (status = Minor)

On the maps, the icons for the monitored node (status = Minor) and its interfaces (status = **Unknown**) are updated:



## Temperature Sensor is Out of Range

A **Temperature Sensor is Out of Range** incident indicates the Source Node's temperature sensor is either too hot or too cold.

A **Temperature Sensor is Out of Range** incident is generated with Severity set to **Critical**.

On the Source Node form, information on the following tabs is updated:

- **Correlated Children**
- **Status**
- **Conclusions**

The Correlated Children tab includes any associated traps.

On the map, the Causal Engine sets the color of the Source Node to yellow.

## Voltage is Out of Range

A **Voltage is Out of Range** incident indicates the specified voltage on one of the Source Node's power supplies is out of range.

A **Voltage is Out of Range** incident is generated with Severity set to **Critical**.

On the Source Node form, information on the following tabs is updated:

- **Correlated Children**
- **Status**
- **Conclusions**

The Correlated Children tab includes any associated traps.

On the map, the Causal Engine sets the color of the Source Node to yellow.

## Interpret Service Impact Incidents

Service Impact incidents indicate a relationship between incidents in which a network service is affected by other incidents. The Service Impact incident helps to identify the service that is affected. Any associated incidents that have contributed to the reason for the Service Impact appear under the Conclusions tab for the Service Impact incident.

A Service Impact incident is indicated using the incident Correlation Nature attribute.

**Note:** NNMi determines the Correlation Nature for an incident.

---

*NNMi Advanced.* As an example of a Service Impact incident and its relationship between additional incidents: an Interface Down incident on an interface that is part of a Router Redundancy Group can effect the integrity of a Router Redundancy Group that is part of an HSRP service. To continue the example, A Router Redundancy Group Degraded incident might be the Service Impact incident used to indicate there is a problem with your HSRP service. The Interface Down incident would appear under the Conclusions tab for the Router Redundancy Degraded incident to indicate that it is part of the reason the Router Redundancy Group (and subsequent HSRP service) has become degraded.

NNMi provides the following incidents whose Correlation Nature is Service Impact:

- ["Primary Device in Router Redundancy Group Switched \(NNMi Advanced\)" \(on page 198\)](#)
  - ["No Primary Device in Router Redundancy Group \(NNMi Advanced\)" \(on page 198\)](#)
  - ["Multiple Primary Devices in Router Redundancy Group \(NNMi Advanced\)" \(on page 198\)](#)
  - ["No Secondary Device in Router Redundancy Group \(NNMi Advanced\)" \(on page 198\)](#)
  - ["Multiple Secondary Devices in Router Redundancy Group \(NNMi Advanced\)" \(on page 199\)](#)
  - ["Router Redundancy Group Degraded \(NNMi Advanced\)" \(on page 199\)](#)
-

**Note:** NNMi determines the Correlation Nature for an incident.

See "[Router Redundancy Group View \(NNMi Advanced\)](#)" (on page 24) for more information about Router Redundancy Groups.

---

### **Primary Device in Router Redundancy Group Switched (NNMi Advanced)**

A Primary Device in Router Redundancy Group Switched incident means NNMi determined a primary role (for example, HSRP Active or VRRP Master) moved from one device to another in a Router Redundancy Group.

**Note:** The group is routing packets properly.

Reasons for this incident include one or more of the following:

- A router or interface in the Router Redundancy Group has gone down.
- A tracked object (interface or IP address) in the Router Redundancy Group has gone down.

When a Primary Device in Router Redundancy Group Switched incident is generated, the Router Redundancy Group maintains its current status.

A Primary Device in Router Redundancy Group Switched incident has Severity set to **Critical**.

### **No Primary Device in Router Redundancy Group (NNMi Advanced)**

A No Primary Device in Router Redundancy Group incident means NNMi determined no primary device (for example, HSRP Active or VRRP Master) is identified in a Router Redundancy group.

This typically indicates one of the following:

- Too many routers are down.
- Protocol specific communication between routers in the group is malfunctioning.

A No Primary Device in Router Redundancy Group incident has Severity set to **Critical**.

### **Multiple Primary Devices in Router Redundancy Group (NNMi Advanced)**

A Multiple Primary Devices in Router Redundancy Group incident means NNMi determined multiple primary devices (for example, HSRP Active or VRRP Master) are identified in a Router Redundancy Group.

This incident typically indicates that protocol specific communication between routers in the group is malfunctioning.

A Multiple Primary Devices in Router Redundancy Group incident has Severity set to **Critical**.

### **No Secondary Device in Router Redundancy Group (NNMi Advanced)**

A No Secondary Device in Router Redundancy Group incident means NNMi determined no secondary device (for example, HSRP Standby or VRRP Backup) is identified in a Router Redundancy Group.

This incident typically indicates the following:

- Protocol-specific communication between routers in the group is malfunctioning.
- The group is routing packets properly because a single primary device has been identified.

A No Secondary Device in Router Redundancy Group incident has Severity set to **Warning**.

### **Multiple Secondary Devices in Router Redundancy Group (NNMi Advanced)**

A Multiple Secondary Devices in Router Redundancy Group incident means NNMi determined more than one secondary device (for example, HSRP Standby) is identified in a Router Redundancy Group.

**Note:** This incident applies to only Router Redundancy Groups using the HSRP protocol. VRRP allows multiple secondary (VRRP Backup State) routers.

This incident typically indicates that protocol specific communication between routers in the group is malfunctioning.

A Multiple Secondary Devices in Router Redundancy Group incident has Severity set to **Critical**.

### **Router Redundancy Group Degraded (NNMi Advanced)**

This incident only occurs in Router Redundancy Groups using the HSRP protocol and with more than two members.

**Note:** The group is routing packets properly.

A Router Redundancy Group Degraded incident means NNMi determined the following:

- The Router Redundancy Group has a primary and secondary device.
- The remaining devices in the group are not in an expected protocol-specific state. For example, in HSRP, devices other than the Standby and Active devices are expected to be in the "Listen" state.
- Protocol-specific communication between routers in the group is malfunctioning.

A Router Redundancy Group Degraded incident has Severity set to **Warning**.

### **Interpret Threshold Incidents (NNM iSPI Performance for Metrics)**

*(NNM iSPI Performance for Metrics)* If the NNMi administrator configures performance measurement thresholds, NNMi monitors interfaces for acceptable operations ranges or threshold violations. NNMi can be configured to create incidents when performance outside the acceptable range is detected. When the performance returns to within an acceptable range, NNMi closes the incident. NNM iSPI Performance for Metrics software provides exceptions reports to track the frequency of threshold violations.

The following table describes possible threshold incidents.

**Note:** Performance thresholds can affect the status of an interface, connection, or node. For example, if an interface error rate is high, the interface status becomes **Critical**. NNMi's Causal Engine returns the node status of **Warning** for any nodes whose interfaces are outside one or more threshold boundaries.

**Tip:** See ["Incident Form" \(on page 134\)](#) for more information about each performance measurement.



### Threshold Incidents

Performance Measurement	Interface Performance State	Message	Incident Severity
Input Utilization	HIGH	Interface Input Utilization High	Critical
	LOW	Interface Input Utilization Low	Minor
	NONE	Interface Input Utilization None	Major
Output Utilization	HIGH	Interface Output Utilization High	Critical
	LOW	Interface Output Utilization Low	Minor
	NONE	Interface Output Utilization None	Major
Input Error Rate	HIGH	Input Error Rate High	Critical
Output Error Rate	HIGH	Output Error Rate High	Critical
Input Discard Rate	HIGH	Input Discard Rate High	Critical
Output Discard Rate	HIGH	Output Discard Rate High	Critical

### Input and Output Utilization Incidents (*NNM iSPI Performance for Metrics*)

Utilization incidents are available if NNM iSPI Performance for Metrics software is installed and your administrator configured performance measurement thresholds.

Input and output utilization incidents enable you to identify interfaces that are over- or under-utilized.

You receive input and output utilization incidents when performance is not within the allowable range set by your administrator. Reasons for setting utilization thresholds include:

- Monitor for under-utilization which wastes money
- Monitor for over-utilization, which may result in performance bottlenecks or service provider surcharges (over a pre-specified percentage)

The severity of utilization incidents depends on whether the measured value is over or under the allowable range. The following table describes the meaning of HIGH, NOMINAL, LOW, and NONE.

Utilization Value	Description	Incident Severity
NONE	The measured value is zero.	Minor
LOW	The measured value is less than the allowable range.	Minor
NOMINAL	The measured value is within the allowable range. This incident cancels any related HIGH, LOW, or NONE incidents.	Not applicable. No incident is generated.
HIGH	The measured value is greater than the allowable range	Critical

Information under the following Incident tabs is updated:

- Correlated Parents
- Correlated Children
- Custom Attributes

The following table describes a combination of conclusions leading to utilization errors. These appear in the Conclusions lists on the associated interface and connection or node forms.

#### **Possible Conclusion Combinations for Utilization Incidents (Interface and Connection)**

Form	Conclusion	Status
Interface	InterfaceOutputUtilizationHigh	Critical
Connection	SomeConnectionThreshold ValuesHigh	Minor

#### **Possible Conclusion Combinations for Utilization Incidents (Interface and Node)**

Form	Conclusion	Status
Interface	InterfaceOutputUtilizationHigh	Critical
Node	SomeInterfacesOutsideThresholdBoundariesInNode	Minor

### **Input and Output Error Rate Incidents (*NNM iSPI Performance for Metrics*)**

Error rate incidents are available if NNM iSPI Performance for Metrics software is installed and your administrator configured performance measurement thresholds.

Input and output error rate incidents allow you to identify interfaces that are dropping data.

You receive input and output error rate incidents when an error rate threshold is not within the allowable range set by your administrator. For example, the error rate must not exceed 10 percent. Reasons for setting error rate thresholds include:

- Check for corrupted data packets
- Detect configuration mismatches
- Detect faulty hardware

Only error rates that exceed the allowable range generate an incident. The severity of error rate incidents is **Critical**.

Information on the following Incident tabs is updated:

- Correlated Parents
- Correlated Children
- Custom Attributes

The following table describes a combination of conclusions leading to error rate incidents. These appear in the Conclusions lists on the associated interface and connection or node forms.

**Possible Conclusion Combinations for Error Rate Incidents (Interface and Connection)**

Form	Conclusion	Status
Interface	InterfaceInputErrorRateHigh	Critical
Connection	SomeConnectionThreshold ValuesHigh	Minor

**Possible Conclusion Combinations for Error Rate Incidents (Interface and Node)**

Form	Conclusion	Status
Interface	InterfaceInputErrorRateHigh	Critical
Node	SomeInterfacesOutsideThresholdBoundariesInNode	Minor

**Input and Output Discard Rate Incidents (*NNM iSPI Performance for Metrics*)**

(*NNM iSPI Performance for Metrics*) Prerequisite, your NNMi administrator configured performance measurement thresholds.

Input and output discard rate incidents enable you to identify interfaces that have transmission buffer overflows or are bottlenecks.

You receive input and output discard rate incidents when a discard rate is not within the allowable range set by your administrator. For example, the discard rate must not exceed 10 percent. Reasons for setting discard rate thresholds include:

- Check for large data packets
- Monitor bottlenecks
- Detect faulty hardware

Only discard rates that exceed the allowable range generate an incident. The severity of discard rate is **Critical**.

Information on the following Incident tabs is updated:

- Correlated Parents
- Correlated Children
- Custom Attributes

The following table describes a combination of conclusions leading to discard rate incidents. These appear in the Conclusions lists on the associated interface and connection or node forms.

**Possible Conclusion Combinations for Discard Rate Incidents (Interface and Connection)**

Form	Conclusion	Status
Interface	InterfaceInputDiscardRateHigh	Critical
Connection	SomeConnectionThreshold ValuesHigh	Minor

### Possible Conclusion Combinations for Discard Rate Incidents (Interface and Node)

Interface	InterfaceInputDiscardRateHigh	Critical
Node	SomeInterfacesOutsideThresholdBoundariesInNode	Minor

## Find a Node

As part of the investigation and diagnosis process, you might want to access the details for a specific node. One way is to use the **Tools** → **Find Node** option. This option is particularly useful when you want to search for a node by any of its IP addresses.

You can find a node based on the values described in the following table.

### Find Node Attribute

Possible Values	Description
Hostname	The fully-qualified DNS name or the IP address, whichever is available. (This is the name that appears in the Hostname field on Node forms.)
IP address of any interface	The IP address for any interface on the node.
System name	The full system name; for example <code>cisco5500.abc.xyz.com</code> that is obtained from the node's SNMP agent. (This is the name that appears in the System Name field on Node forms.)
Name	The type of name your administrator has configured using the <b>Node Name Resolution</b> attribute during discovery configuration. For example, this might be the short DNS name, or short system name. (This is the name that appears in the Name field on Node forms.)

### To find a node using the node's hostname, IP address, system name, or name attribute value:

1. From the console, select **Tools** → **Find Node**.
2. At the **Node Name** field of the **Specify Node** dialog, enter the hostname, an IP address, system name, or Name value for the node of interest.

**Note:** Names are case-sensitive.

3. Click **Find**.

NNMi searches the database to find a matching value using each of the attributes listed in the preceding table.

NNMi shows the node form for the node you specified. If no node is found, NNMi shows an error message. If multiple nodes are found, NNMi shows the first node it finds.

See "[Access Node Details](#)" (on page 130) for more information about the kind of information that appears in the Node form. See [Access More Details \(Quick View and Forms\)](#) for a description of additional ways to access node details.

## Find the Attached Switch Port

This tool helps you investigation and diagnosis problems. You might need to determine the switch to which a problem node is connected. For example, if a node in your network has a potential virus, you want to identify the switch to which it is connected so that you can prevent the virus from moving to other nodes in your network. One way to identify a switch port attached to a problem node is to use the **Tools** → **Find Attached Switch Port** option.

You can find the attached switch and the port that is connected from the switch to the problem node using any of the values described in the following table. Each of these values is for the problem node.

**Note:** The node whose information you provide does not have to be discovered by NNMi.

### Find Attached Switch Port Attribute

Possible Values	Description
Hostname	See the Hostname attribute value on the <a href="#">"Node Form" (on page 28)</a> of the node that is attached to the switch you are trying to identify. This value might be an all-lowercase DNS hostname or an IP address.  <b>Note:</b> What is entered here is case-sensitive. NNMi converts the fully-qualified DNS hostnames to all lowercase when storing the discovered hostname in the NNMi database.
IP address of any interface	The IP address for any interface in the node that is attached to the switch you are trying to identify.
MAC address	The MAC (Media Access Control) address of any interface in the node that is attached to the switch you are trying to identify.

### To identify the port number of the switch to which a node is connected:

1. From the console, select **Tools** → **Find Attached Switch Port**.
2. At the **End Node Name** field of the **Specify Hostname, IP Address, or MAC Address** dialog, enter the hostname, an IP address, or the interface MAC address for the node of interest.
3. Click **Find**.

NNMi searches the database to find a matching value using the hostname, IP address, or MAC address provided.



NNMi shows the hostname of the node and the name of the node's interface or port number. Click the node name to open the Node form for the switch attached to the node you specified. Click the interface name to open the Interface form. If the node or attached switch port is not found, NNMi shows an error message. If multiple attached switches are found, NNMi shows the first attached switch it finds.

See ["Access Node Details" \(on page 130\)](#) for more information about the kind of information that appears in the Node form. See [Access More Details \(Quick View and Forms\)](#) for a description of additional ways to access node details.

## Display End Nodes Attached to a Switch

This action helps you investigation and diagnosis problems. You might need to determine the end nodes attached to a switch. For example, if you need to upgrade a switch, you might need to check which servers are attached to the switch so that you can fill out the change request properly.

To display the end nodes attached to a switch using the NNMi console Actions menu, do one of the following:

1. Navigate to the view or form of interest and select the switch whose attached end nodes you want to display.
  - **Navigate to a table view and select a switch:**
    - i. From the workspace navigation panel, select the workspace of interest; for example, **Inventory**.
    - ii. Click the view that contains the switch whose attached end nodes you want to display; for example **Nodes**.
    - iii. From the table view, click the  selection box in the row that represents the switch of interest.
  - **Navigate to a map view and select a switch:**
    - i. Navigate to the table view.
    - ii. From the table view, click the  selection box in the row that represents the switch of interest.
    - iii. Select **Actions** → **Layer 2 Neighbor View, Layer 3 Neighbor View, Node Group Map, or Path View**.
    - iv. In the map, click the map symbol representing the switch of interest.
  - **Navigate to a form:**
    - i. From a table view, click the  Open icon in the row that represents the switch of interest.
    - ii. From a map view, click the switch of interest on the map and click the  Open icon.
2. Select **Actions** → **Show Attached End Nodes**.

NNMi displays the following for each end node that it determines is attached to the switch:

- Resolved hostname
- MAC address of the connected interface
- IP address

Note the following:

- If the end node does not have a resolvable hostname, NNMi repeats the node's IP address.
- If NNMi is unable to locate any information about end nodes attached to the selected switch, NNMi displays a message that it was unable to locate any entries for the switch.

3. Click any object name link to open the form for the selected object.

**Note:** If the object name appears without a link, this indicates NNMi has not discovered the node or interface.

### Related Topics

---

["Find the Attached Switch Port" \(on page 204\)](#)

## Test Node Access (Ping)

You can verify that a node or IP address is reachable using the ping command from the NNMi console **Actions** menu.

**Note:** NNMi uses the packet size used by the current operating system.

**From an incident view:**

1. Click the  selection box that precedes the incident whose source node you want to ping.
2. Select **Actions** → **Ping (from server)**.

**Note:** NNMi pings the source node of the incident. It does not ping the source object. For example, if the incident is related to an interface, NNMi pings the node on which the interface resides, not the interface itself.

**From other views or forms:**

1. Navigate to the view or form of interest and select the node or IP address you want to ping.



**To navigate to a table view and select a node:**

- a. From the workspace navigation panel, select the workspace of interest; for example, **Inventory**.
- b. Click the view that contains the node or IP address that you want to verify is reachable; for example **Nodes**.
- c. From the table view, click the  selection box in the row that represents the node or IP address.

**To navigate to a map view and select a node:**

- a. Navigate to the table view.
- b. From the table view, click the  selection box in the row that represents the node or IP address.
- c. Select **Actions** → **Layer 2 Neighbor Views**, **Layer 3 Neighbor Views** or **Path View**.
- d. In the map, click the map symbol representing the node of interest.

**To navigate to a form:**

- a. From a table view, click the  Open icon in the row that represents the node or IP address of interest.
  - b. From a map view, click the node of interest on the map and click the  Open icon.
2. Select **Actions** → **Ping (from server)**

NNMi displays the ping results, including reply times and ping statistics.

## Find the Route (traceroute)

When investigating and diagnosing network problems, you might want to trace the route path using the traceroute command. Using traceroute also lets you identify bottlenecks along the destination path

provided. You can access the traceroute command from the NNMi console Actions menu.

**Note:** You can also use Path View to display the routing path between two nodes that have IPv4 addresses. See ["Path Between Two Nodes that Have IPv4 Addresses" \(on page 114\)](#) for more information.

**Note:** The starting node is the NNMi management server on which you are running the trace route command.

**To access the trace route command:**

1. From an incidents view, select the incident whose source node on which you want to use trace route.  
Or from a nodes view, select the node on which you want to use trace route.

2. Select **Actions** → **Trace Route (from server)**.

NNMi displays the output from trace route, including the lists of routers that are traversed to reach the destination node.



**To navigate to a table view and select a node:**

1. From the workspace navigation panel, select the workspace of interest; for example, **Inventory**.
2. Click the view that contains the node whose communication settings you want to check; for example **Nodes**.
3. From the table view, click the  selection box that precedes the node whose configuration you want to check.

**To navigate to a map view and select a node:**

1. Navigate to the table view.
2. From a table view, click the  selection box that precedes the node of interest.
3. Select **Actions**.
4. From the drop-down menu, select the map view of interest.
5. From the map view, click the node whose configuration you want to check.

**To navigate to a form:**

1. From the table view, click the  Open icon that precedes the node of interest.
2. From a map view, click the node of interest on the map and click the  Open icon.

## Establish Contact with a Node (telnet)

When investigating and diagnosing network problems, you might need to establish a connection to a node to view or change configuration information. You can establish a connection to a node using the telnet command from the NNMi console Actions menu.

**Note:** To access telnet from Microsoft Internet Explorer, you must first tune the FEATURE\_DISABLE\_TELNET\_PROTOCOL registry entry as described in: <http://msdn2.microsoft.com/en-us/library/ms537169.aspx>. More specifically, you will want to add the following registry key: [HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_DISABLE\_TELNET\_PROTOCOL] to have the value: "iexplore.exe"=dword:00000000. HP recommends that you back up your registry before making any changes. For information about how to back up and edit your registry, see the Microsoft Knowledge Base article at <http://support.microsoft.com/kb/322756>.



**To establish contact with a node using telnet:**

**From an incident view:**

1. Click the  selection box that precedes the incident whose source node you want telnet.
2. Select **Actions** → **Telnet (from client)**.

**Note:** NNMi telnets the source node of the incident. It does not telnet the source object. For example, if the incident is related to an interface, NNMi telnets to the node on which the interface resides, not to the interface itself.

**From other views or forms:**

1. Navigate to the view or form of interest and select the node to which you want to telnet.



**To navigate to a table view and select a node:**

- a. From the workspace navigation panel, select the workspace of interest; for example, **Inventory**.
- b. Click the view that contains the node whose communication settings you want to check; for example **Nodes**.
- c. From the table view, click the  selection box that precedes the node whose configuration you want to check.

**To navigate to a map view and select a node:**

- a. Navigate to the table view.
- b. From a table view, click the  selection box that precedes the node of interest.
- c. Select **Actions**.
- d. From the drop-down menu, select the map view of interest.
- e. From the map view, click the node whose configuration you want to check.

**To navigate to a form:**

- a. From a table view, click the  Open icon that precedes the node of interest.
  - b. From a map view, click the node of interest on the map and click the  Open icon.
2. Select **Actions** → **Telnet (from client)**.

NNMi displays a browser window and a telnet window.

## Check Status Details for a Node Group

When diagnosing and troubleshooting problems, you might want to check the status for only a particular set of nodes. Your network administrator is able to group sets of nodes into Node Groups. An example Node Group could be all important Cisco routers, or all routers in a particular building. See [About Node and Interface Groups](#) for more information about how your administrator sets up Node Groups. See [Filter by Node or Interface Group](#) for more information about filtering views using Node Groups.

You can view Node Group status information using the Nodes Group View or Node Group Map view. See ["Node Groups View \(Inventory\)" \(on page 25\)](#) or ["Node Groups View \(Monitoring\)" \(on page 128\)](#) as well

as "[Node Group Maps](#)" (on page 99) for more information. When you want more details about the number of nodes that have a particular status within the Node Group, use the **Actions** menu.

**Note:** The Status Details window automatically refreshes Status Detail information every 5 minutes.

**To check the status details for a Node Group using a table view:**

1. Navigate to the Node Groups view of interest. For example, select **Monitoring** → **Node Groups**.
2. Click the selection box that precedes the Node Group of interest.
3. Select **Actions** → **Status Details**.

For the Node Group selected, NNMi shows the following information:

- Node Group name
- Overall Node Group status
- Number of nodes in the group with each possible status
- Percentage of nodes in the group with each possible status

**To check the status details for a Node Group using a map view:**

1. From the workspace navigation panel, select the **Inventory** or **Monitoring** workspace.
2. Select **Node Groups**.
3. In the Node Group view, click the  selection box that precedes the Node Group of interest.
4. Select **Actions** → **Node Group Map**.

See [About Map Status](#) for more information about status colors.

## Accessing NNM 6.x and 7.x Features

Your NNMi administrator might configure NNMi so that you are able to view incidents that are being forwarded from an NNM 6.x or 7.x management station.

If your NNMi administrator has configured any NNM 6.x or 7.x management stations, you are able to view this information using the **Inventory** workspace. The **Management Stations** view in the **Inventory** workspace is useful for identifying all of the NNM 6.x or 7.x management stations that might be forwarding incidents to your NNMi incident views. See "[Management Stations View \(Inventory\)](#)" (on page 26) for more information.

If an NNM 6.x or 7.x management station has been configured, you are also able to access the following NNM 6.x or 7.x features from the NNMi **Actions** menu:

**Note:** You can only launch the 6.x/7.x oww action if oww is running on the NNM 6.x/7.x management station.

From Incident Views

- **Actions** → **6.x/7.x Neighbor View**
- **Actions** → **6.x/7.x Details**
- **Actions** → **6.x/7.x oww**

From Management Station Views

- **Actions** → **6.x/7.x Home Base**
- **Actions** → **6.x/7.x oww**

- **Actions** → **6.x/7.x Launcher**
- **Actions** → **SNMP Viewer**
- **Actions** → **Alarms**

**Note:** You can only access NNM 6.x/7.x features by selecting incidents generated from NNM 6.x/7.x events.

## Checking the Status of NNMi

To confirm that NNMi is running properly, check NNMi status. If one or more of the NNMi processes or services are not running, contact your NNMi administrator to have the process or service restarted.

### To check the health of NNMi:

1. From the NNMi console, select **Tools** → **NNM Status**.

NNMi displays a list showing the status of each process and service.

Each process and service should be running. If one is not, contact your NNMi administrator.

You can also check the health of the State Poller.

### To check the health of the State Poller:

1. From the NNMi console, select **Help** → **About HP Network Node Manager i-series**.

NNMi displays the status of the State Poller as well as State Poller collection and queue information.

## Appendix A: Glossary Terms

---

### A

---

#### **Anycast Rendezvous Point IP Address**

Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

### L

---

#### **Layer 2**

Refers to the Data Link layer of the multilayered communication model, Open Systems Interconnection (OSI). The Data Link layer moves data across the physical links in the network. The switches and bridges are devices that redirect data messages at the layer 2 level, using the destination Media Access Control (MAC) address to determine where to direct the message.

#### **Layer 3**

Refers to the Network layer of the multilayered communication model, Open Systems Interconnection (OSI). The Network layer is concerned with knowing the address of the neighboring nodes in the network, selecting routes and quality of service, and recognizing and forwarding incoming

messages to local host domains. The router and switch-router are the devices that redirect data messages at the Layer 3 level. Everything in a subnet is connected at the Layer 3 (IP) level.

#### **Link Aggregation**

A Link Aggregation is comprised of an Aggregator Link, Aggregator Interface, and the physical interfaces and connections that they represent. An Aggregator Link object represents many-to-many physical connections. For example, two nodes might be connected with four physical connections. These four physical connections are depicted as a single Aggregator Link object using a thick line on the Layer 2 Neighbor View map. The interface depicted at each end of the Aggregator Link object is an Aggregator Interface object. An Aggregator Interface object represents the collection of physical interfaces for one end of an Aggregator Link.

#### **loopback address**

The address associated with the loopback interface. The loopback interface is a virtual interface on a device that provides a route for internal communication. Many vendors provide a specially configured

---

loopback for management purposes. Exact details of how loopbacks are configured varies by vendor and model. See each device's documentation for details. NNMi identifies these loopback addresses by using IfType 24, softwareloopback from the IANA ifType-MIB.

## Appendix B: Index

<b>A</b>	
abnormal network behavior, troubleshooting	13
accessing	
device details	27, 56
node details	130
old NNM features	14, 209
Path View	114
performance data	118
problem devices	129
related	
incidents	130
traceroute command	206
Actions menu	
accessing	
maps	99-100, 158, 208
performance data	118
investigating devices	129
monitoring configuration settings	178
Path View	114
running diagnostics	46-47, 147
troubleshooting network problems	104, 112, 177
unassigning incidents	150
updating lifecycle states	157
active paths	116
adding	
maps	103
node	
capabilities	38
subnet notes	113
Additional Filters tab	90, 96
Additional Node form	91
Additional Nodes tab	90
Address Disabled	182
Address Not Responding	182
addresses	
configuration settings	178
customizing views	24
disabled	182
identifying non-responsive	124
not	
responding	182
polling policy	73, 78
administrative states	125
Advanced, NNMi	
Aggregator Interface Degraded	183
Aggregator Interface Down	184
Aggregator Link Degraded	185
Aggregator Link Down	185
enhanced Path View	118
interface capabilities	67
Interface form	65, 71
Layer 2 Connection form	109
Management Stations view	26
Multiple Primary Device	198
Multiple Secondary Device	199
No Primary Device	198
No Secondary Device	198
node capabilities	36
Primary Device	198
RAMS	114
Router Redundancy Group	
form	80, 84-85
view	24
Router Redundancy Group Degraded	199
Router Redundancy Member form	80, 83
Service Impact incidents	197

Index: agents, SNMP – capabilities

Tracked Objects form	84	Layer 2 Connection form	106-109, 111
Virtual IP Addresses form	85	Lifecycle State	154
agents, SNMP		Management Stations form	97
not responding	196	Node Capability form	38
Aggregator Interface Degraded incidents	183	Node Component form	40, 42, 44-45
Aggregator Interface Down incidents	184	Node Custom Attributes form	39
Aggregator Link Degraded incidents	185	Node Device Filter form	89
Aggregator Link Down incidents	185	Node Diagnostic Results form	47
alerts, network	181	Node form	28, 32-35, 39-40, 46, 48, 50
annotating information	13	Node Group form	88-90, 93
Assigned To lookup field	150	Node Group Hierarchy form	92
assigning		nodes	203
incidents	149-150	Port form	87
attached switch ports, finding	204	RCA Active	154
attribute values		Router Redundancy Group form	79-80
Additional Node form	91	Router Redundancy Member form	80, 83
device		SNMP Agent form	50, 54-55
author	59	Tracked Objects form	84
category	59	Virtual IPAddresses form	85
family	58	VLAN form	86
profile	56	attributes	
vendor	58	IP addresses	24
Find Attached Switch Port	204	Notes	151
Health Attribute form	42	Attributes, Custom Incident	143
IfType Filter form	95	Author form	59
IfTypes form	96		
Incident Diagnostic Results form	147	<b>B</b>	
Incident form	134-135, 142, 147-148	broadcast domain, reduced	20
incidents	143	Buffer has Insufficient Capacity or is Malfunctioning incident	186
Interface Capability form	69		
Interface Custom Attributes form	69	<b>C</b>	
Interface form	60, 63-66, 69-73	calculation rules, Path View	116
Interface Group form	94-95	capabilities	
IP Address form	73, 75-76, 78	interface	67
IP Subnet form	113-114	node	36



Capabilities tab		Conclusions tab	
Interface form	66	Interface form	73
Node form	35-36	IP Address form	76
categories		Layer 2 Connection form	109
devices	59	Node Component form	45
incidents	166, 174	Node form	49
Causal Engine	159, 170, 177, 181, 192	SNMP Agent form	54
causes, root		configuration	
connectivity problems	104, 112	monitoring settings	178
incident		verifying device	177
messages	181	configuring	
views	163, 168, 170-171	device profiles	56
checking		connecting to nodes	207
NNMi status	211	connection	
node group status details	208	mesh	104
Child Node Group		Connection Down incident	186
attribute	92	Connection Partially Unresponsive incident	187
displaying	100	connectivity	
Child Node Groups tab	92	troubleshooting problems	104, 112
CIAs	143	viewing network maps	98
Cisco		Correlated Children tab	142
protocols	117	Correlated Parents tab	142
routers	16	Correlation Nature attribute	197
Closed Key Incidents view	168	CPU Utilization is Too High incident	188
colors		creating	
device connections	98	attributes	
status	129	Author	59
commands		Device Category	59
ping	206	Device Family	58
traceroute	117, 206	Device Vendor	58
Component Health		criteria	
tab	40	node down	192
components		Critical Interfaces view	120
Causal Engine	159, 170, 177, 181	Critical Nodes view	121
		Critical status	120, 183-185, 195

Index: custom attributes – displaying

custom attributes		Device Profile form	56
for nodes	39	Device Vendor form	58
Custom Attributes tab	142	devices	
Interface form	69	accessing problem	129
Node form	39	active path	116
Custom Incident Attributes	143	categories	16, 21
Custom Incidents view	159, 173	connections	104
Custom Interfaces view	23	families	58
Custom IP Addresses view	24	identifying	114, 128
Custom Nodes view	23	managed	27
customer network	117	profiles	56
customizing views		types	56
nodes	23	verifying	
		configuration details	177
		status	180
		VLANs	20
		diagnosing network problems	177
		diagnostic results, node	47
		Diagnostics tab	46-47, 147
		diagrams, flow	114
		disabled	
		address	182
		interface	189
		discard rate incidents	202
		discovering networks	15
		updating information	177
		Discovery, Spiral	56
		displaying	
		incidents	130, 158
		key incidents closed	168
		Layer 2 connectivity	104
		Layer 3 connectivity	112
		network connectivity maps	98
		Network Infrastructure Devices Overview map	102
		Node Group map	99-100
<b>D</b>			
database			
deleting objects	16		
determining SNMP Agent attributes	50, 54-55		
SNMP trap limit	195		
defining			
interface groups	94		
degraded aggregator			
interface	183		
link	185		
deleting			
abnormal network behavior	13		
maps	103		
nodes	16		
detecting abnormal network behavior	13		
determining			
problem scopes	129		
Device Category form	59		
Device Family form	58		
Device Filters tab	89		

Node Group Overview map	101	Family	
paths between nodes	114	incidents	173
root cause incidents	170-171	Fan Is Malfunctioning incident	188
category	166	fault management	13
closed	168	features, accessing old	14, 209
family	167	filtering	
lifecycle state	169	incidents	133
open	164	categories	166
priority	165	custom	173
unassigned	163	families	167
Routers map	103	NNM 6.x/7.x events	174
Switches map	103	priorities	165
views	20	severities	164
domain, reduced broadcast	20	SNMP traps	175
down		interface	
aggregator		administrative state	125
interface	184	custom	23
link	185	groups	16, 25
connection	186-187, 194	operational state	126
interface	188	status	125
node	192, 194	IP addresses	24, 126
		node groups	16, 25
		views	15, 21-22, 124, 169
		filters	
		additional	96
		interface	
		groups	95
		types	95
		Find Attached Switch Port option	204
		finding	
		attached switch port	204
		nodes	203
		route path	206
		flow	
		diagrams	114
<b>E</b>			
enhanced Path View	118		
error rate incidents	201		
errors, Path View	118		
expanding child in node group map	99		
Express Forwarding, Cisco	117		
extending capabilities			
node	38		
<b>F</b>			
Failover in Router Redundancy Group message	198		
families			
filtering views	167		

forms		Tracked Objects	84
Additional Node	91	updating lifecycle state	157
Author	59	Virtual IPAddresses	85
Custom Incident Attribute	143	VLAN	86
Device Category	59		
Device Family	58	<b>G</b>	
Device Profile	56	General tab	32, 63, 135
Device Vendor	58	Global Load Balancing, Cisco	117
Health Attribute	42	groups	
IfType Filter	95	defining	
IfTypes	96	interface	94
Incident	134-135, 142, 147-148, 183-185		
Incident Diagnostic Results	147	<b>H</b>	
Interface	60, 63-66, 69-73	Health Attribute	
Interface Capability	69	form	42
Interface Custom Attributes	69	tab	42
Interface Group	94-96	health, component	40
invoking actions	204	health, network	
IP Address	73, 75-76, 78	verifying	211
IP Subnet	113-114	historical information	13
Layer 2 Connection	106-109, 111	HSRP	
Management Stations	97	nodes	118
navigating	177, 206-207		
Node	28, 32-36, 39-40, 46, 48-50	<b>I</b>	
Node Capability	38	ICMP	
Node Component	40, 42, 44-45	displaying root cause incidents	170
Node Custom Attributes	39	incidents	159
Node Device Filter	89	ping command	182
Node Diagnostic Results	47	icons	
Node Group	88-90, 92-93	Interface form	70
Node Group Hierarchy	92	node status	44
Port	87	severity	132
Router Redundancy Group	79-80, 84-85	identifying	
Router Redundancy Member	80, 83	critical nodes	121
SNMP Agent	50, 54-55	devices	114

interface performance	127	displaying	
IP addresses	19, 24, 126	map	158
networks		Fan is Malfunctioning	188
interfaces managed by NNMi	17	input and output	
management domain	19	discard rate	202
nodes		error rate	201
by status	124	utilization	200
managed	16	Interface Disabled	189
non-normal		Interface Down	188
interfaces	122	Interface Unmanageable	190
nodes	122	key	161
non-responsive addresses	124	key views	160
IfType Filter		lifecycle	154, 157
form	95	monitoring	132
tab	95	No Primary Device in Router Redundancy Group	198
IfTypes		No Secondary Device in Router Redundancy Group	198
form	96	Node Down	192
important nodes		Node or Connection Down	194
critical status	187, 192	Non-SNMP Node Unresponsive	195
Incident Diagnostic Results form	147	Number of SNMP Traps Persisted in the Database has Reached	
Incident form	134-135, 142, 147-148, 183-185	open	160
incidents		open root cause	171
Address Not Responding	182	organizing	133
Aggregator Interface Degraded	183	owning	149
Aggregator Interface Down	184	Power Supply is Malfunctioning	196
Aggregator Link Degraded	185	Service Impact	197
Aggregator Link Down	185	SNMP Agent Not Responding	196
assigning	149-150	Temperature Sensor is Out of Range	196
attributes	143	threshold	199
Buffer has Insufficient Capacity or is Malfunctioning		tracking	
Connection Down	186	progress	157
Connection Partially Unresponsive	187	troubleshooting	134-135, 142, 147-148, 172, 181
CPU Utilization is Too High	188	unassigning	150
		updating	151

Index: Incidents by Family view – Interface form

views	159	filtering	
categories	166	administrative states	125
custom	173	operational states	126
families	167	status	125
lifecycle state	169	identifying non-normal	122
management stations	26	monitoring	
NNM 6.x/7.x events	174	views	120
priorities	165	notes	17
related	130	out-of-box	
root cause	170	capabilities	67
router redundancy group	24	performance states	70
severities	164	polling policy	60
SNMP traps	175	status	17
Voltage is Out of Range	197	viewing	
Incidents by Family view	173	all	17
Incidents tab		non-normal	122
Interface form	71	Interface by Administrative State view	125
IP Address form	75	Interface by IfType view	22
Layer 2 Connection form	108	Interface Capability form	69
Node Component form	44	Interface Custom Attributes form	69
Node form	48	Interface Disabled incident	189
Router Redundancy Group form	85	Interface Down incident	188
SNMP Agent form	55	Interface form	60
input		Capabilities tab	66
discard rate	70, 202	Conclusions tab	73
error rate	70, 201	Custom Attributes tab	69
utilization	70, 200	General tab	63
insufficient		Incidents tab	71
buffer capacity	186	Interface Groups tab	70
memory	192	IP Addresses tab	64
interface		Link Aggregation tab	65
configuration settings	178	Performance tab	70
customizing views	23	Registration tab	73
disabled	182	Status tab	72
		VLAN Ports tab	64

Interface Group		IP Addresses tab	
form	94-96	IP Subnet form	114
view	25	Node form	33
interface groups		IP Addresses view	19
defining	94	IP Subnet form	113
filters	16, 25	IP Addresses tab	114
viewing		Registration tab	114
details	25	IP Subnets view	19
Interface Groups tab	70	ipRoute tables	117
Interface Performance view	127	IPv4 addresses	114
Interface Unmanageable incident	190	Island Node Group	88, 158
Interfaces by Operational State view	126	isolating abnormal network behavior	13
Interfaces by Status view	125	iSPIs	
Interfaces tab		NNM iSPI Network Engineering Toolset	
Layer 2 Connection form	107	diagnostics	46-47, 147
Node form	33	incidents	147
Interfaces view	17	nodes	46-47
interpreting threshold incidents	199	traps	176
inventory		NNM iSPI Performance for Metrics	
network	15	CIAs	143
Inventory workspace		Health Attribute form	42
Interfaces view	17	incidents	199-202
Layer 2 Connections view	21	interface groups	25, 94
Management Stations view	14, 209	interfaces	127
Nodes view	16	monitoring	127-128
investigating		configuration	178
network problems	177	node groups	25, 88, 128
invoking actions	204	nodes	25, 40, 88
IP Address form	73, 78	performance issues	118
Conclusions tab	76	NNM iSPI Performance for Traffic	
Incidents tab	75	interface groups	25, 94
Status tab	75	node groups	25, 88, 128
IP Addresses			
tab	64		
IP Addresses by State view	126		
		<b>K</b>	
		Key Incident views	160

key incidents, viewing	161, 164-168	management mode	
		interface	60
		IP addresses	73
		nodes	28
		management network	117
		Management Stations	
		form	97
		view	14, 26, 209
		managing	
		incident assignments	149
		map objects, viewing details	130
		map views	
		checking node group	208
		determining problem scopes	129
		Device Profiles	56
		incidents	158
		invoking actions	204
		monitoring network problems	128
		navigating	177, 180, 206-207
		network connectivity	98, 114
		node groups	128
		status colors	129, 181
		viewing object details	27
		maps	
		Network Infrastructure Devices Overview	102
		Network Overview	102
		Node Group	99-101
		Node Group Overview	101
		Routers	103
		Switches	103
		Maps	
		Island Node Group	158
		memory, insufficient or malfunctioning	192
		mesh connection	104
	<b>L</b>		
LANs, virtual	20, 86		
Layer 2 Connection form	106		
Conclusions tab	109		
Incidents tab	108		
Interfaces tab	107		
Link Aggregation tab	109		
Registration tab	111		
Status tab	108		
Layer 2 Connections view	21		
Layer 2 Neighbors view	98, 104		
Layer 3 Neighbors view	98, 112		
Layer 3 networks	102		
Level 1 Operator role	150		
Level 2 Operator role	150		
lifecycle, incidents	154, 157, 169		
limits			
Path View	117		
SNMP traps in database	195		
Link Aggregation tab			
Interface form	65		
Layer 2 Connection form	109		
local area networks, virtual	86		
logical networks	20		
		<b>M</b>	
MAC-based VLANs	20		
malfunctioning			
buffer	186		
fan	188		
memory	192		
power supply	196		
managed device, viewing details	27		



messages, incidents		management	117
root causes	181	monitoring	
monitoring		health	211
configuration settings	178	problems	120
devices	21	protocol design	98
incidents	132	Network Engineering Toolset	
interface		diagnostics	46-47, 147
administrative states	125	incidents	147
operational states	126	nodes	46-47
network		traps	176
problems	120, 128, 132	Network Infrastructure Devices Overview map	102
node groups	128	Network Overview map	102
Multiple Secondary Devices in Router Redundancy		NNM iSPI Network Engineering Toolset	
multiple		diagnostics	46-47, 147
VLANs	20	incidents	147
Multiple Primary Devices in Router Redundancy Group		nodes	46-47
My Open Incidents view	149, 160	traps	176
		NNM iSPI Performance for Metrics	
		CIAs	143
		Health Attribute form	42
		incidents	199-202
		interface groups	25, 94
		interfaces	127
		monitoring	127-128
		configuration	178
		node groups	25, 88, 128
		nodes	25, 40, 88
		performance issues	118
		NNM iSPI Performance for Traffic	
		interface groups	25, 94
		node groups	25, 88, 128
		NNMi	
		6.x/7.x	
		Events by Category view	174
		Events view	174
navigating			
forms	177, 206-207		
map views	177, 180, 206-207		
maps	100		
table views	177, 180, 206-207		
neighborhood view maps	98		
network			
abnormal behavior	13		
alerts	181		
connectivity maps	98		
customer	117		
discovering	15		
identifying issues	128		
interfaces	17		
inventory	15		
investigating problems	177		

Index: No Primary Device in Router Redundancy Group incident – node groups

features	14, 209	Node Component form	40
viewing incidents	159	Conclusions tab	45
viewing remote management stations	97	Health Attributea tab	42
Advanced		Incidents tab	44
Aggregator Interface Degraded	183	Status tab	44
Aggregator Interface Down	184	Node Custom Attributes form	39
Aggregator Link Degraded incidents	185	Node Device Filter form	89
Aggregator Link Down	185	Node Diagnostic Results form	47
enhanced Path View	118	Node Down incident	192
interface capabilities	67	Node form	28, 32
Interface form	65, 71	Capabilities tab	35-36
Layer 2 Connection form	109	Component Health tab	40
Management Stations view	26	Conclusions tab	49
Multiple Primary Devices	198	Custom Attributes tab	39
Multiple Secondary Devices	199	Diagnostics tab	46
No Primary Devices	198	Incidents tab	48
No Secondary Device	198	Interfaces tab	33
node capabilities	36	IP Addresses tab	33
Primary Device	198	Node Groups tab	39
RAMS	114	Ports tab	35
Router Redundancy Group Degraded	199	Registration tab	50
Router Redundancy Group form	80, 84-85	Status tab	48
Router Redundancy Group view	24	VLAN Ports tab	34
Router Redundancy Member form	80, 83	Node Group form	88-90, 92-93
Service Impact incidents	197	Node Group Hierarchy form	92
Tracked Objects form	84	Node Group map	99
Virtual IP Addresses form	85	displaying	100
checking status	211	positioning nodes	101
CIAs	143	Node Group Overview Map	101
using	13	node groups	
No Primary Device in Router Redundancy Group incident		checking status	208
No Secondary Device in Router Redundancy Group incident		filters	16, 25, 133
Node Capability form	38	maps	128
Node Component configuration settings	178	monitoring	128

viewing		unresponsive	195
details	25	updating status	180
Node Groups		views	16, 121
tab	39	VRRP	118
view	25, 128	Nodes by Device Category view	21
Node or Connection Down incident	194	Nodes by Status view	124
nodes		Nodes view	16
accessing details	130	Non-Normal Interfaces view	122
attributes	203	Non-Normal Nodes view	122
configuration settings	178	Non-Normal Router Redundancy Group view	123
connecting to	207	Non-SNMP Node Unresponsive incidents	195
customizing views	23	Nortel	
device category	16	private interface	22-23, 60
displaying		SNMP interfaces	17
paths between	114	Not Responding Address view	124
errors	118	notes	
filtering		interfaces	17
status	124	nodes	16
finding	203	subnets	113
HSRP	118	Notes attribute	151
identifying		Number of SNMP Traps Persisted in the Database has Reached	
critical	121	<b>O</b>	
non-normal	122	objects	
Layer 2 connectivity	104	viewing	
Layer 3 connectivity	112	device details	27
monitoring		incidents	130
views	120	node details	130
notes	16	open incidents	160
out-of-box		Open Key Incidents by Category view	166
capabilities	36	Open Key Incidents by Family view	167
polling policy	50, 54-55, 177, 180	Open Key Incidents by Priority view	165
saving map locations	101	Open Key Incidents by Severity view	164
selecting	206	Open Key Incidents view	161
status	16	open root cause incidents	171
testing whether reachable	206		

Index: Open Shortest Path First protocol – profiles, device

---

Open Shortest Path First protocol	117	performance	
Open Systems Interconnection model	98	interface	127
operational states	126	Path View issues	118
operator		states	70
roles		Performance tab	70
Level 1	150	ping command	182, 206
Level 2	150	polling policy	
organizing incidents	133	address	73, 78
OSI model	98	interface	60
out-of-box		node	50, 54-55, 177, 180
CIAs	143	Port form	87
interface		ports	
capabilities	67	details	87
node		finding attached switch	204
capabilities	36	trunk	86
views	15, 120, 159-160	Ports tab	
out of range		Node form	35
temperature sensor	196	VLAN form	86
voltage	197	position nodes on group map	101
output		Power Supply is Malfunctioning incident	196
discard rate	70, 202	priority, open root cause	165
error rate	70, 201	problems	
utilization	70, 200	accessing devices	129
owning incidents	149	determining scope	129
		incidents	132, 172
<b>P</b>		interface	104
parent node group	92	investigating network	177
Path View	114	monitoring network	120
calculation rules	116	node down	192
enhanced	118	root cause	
limitations	117	messages	181
performance issues	118	views	170
paths		subnets	112
displaying between nodes	114	profiles, device	56
finding route	206		

---

progress		results	
incident	157	Path View	116
protocols		roles	
network	98	operator	
router	117	Level 1	150
VLAN	20	Level 2	150
pseudo interfaces	23	updating incidents	134
		Root Cause Incidents view	170-171
		root cause messages	
		Failover in Router Redundancy Group	198
		Multiple Primary Devices in Router Redundancy Group	198
		Multiple Secondary Devices in Router Redundancy Group	199
		No Primary Device in Router Redundancy Group	198
		No Secondary Device in Router Redundancy Group	198
		Router Redundancy Group Degraded	199
		root causes	
		connectivity problems	104, 112
		incident	
		messages	181
		views	159, 163-171
		route path, finding	206
		Router Redundancy Group	
		form	79-80, 84-85
		root cause message	198
		view	24, 123
		Router Redundancy Group Degraded incident	199
		Router Redundancy Member	
		configuration settings	178
		form	80, 83
		tab	80
		routers	
		Cisco	16
		identifying issues	128
		monitoring	116
		protocols	117
<b>Q</b>			
Quick Filter	21-22, 124-126, 164, 166-167, 169		
Quick View	27, 130		
<b>R</b>			
RAMS data and Path View	118		
ranges			
temperature sensor	196		
voltage	197		
RCA Active attribute	154		
RCA messages			
Failover in Router Redundancy Group	198		
Multiple Primary Device in Router Redundancy Gr			
Multiple Secondary Devices in Router Redundanc			
No Primary Device in Router Redundancy Group1			
No Secondary Device in Router Redundancy Gro			
Router Redundancy Group Degraded	199		
Registration tab	148		
Interface form	73		
IP Subnet form	114		
Layer 2 Connection form	111		
Node form	50		
SNMP Agent form	55		
related incidents, displaying	130		
reporting performance	118		
resolved root cause incidents	168		

---

subnet	112	State Poller	
Routers		checking health	211
map	103	service	56
rules, path calculation	116	states	
		administrative	125
		operational	126
		performance	70
		status	
		colors	129
		filtering interface	125
		node groups	93
		nodes	124
		verifying	
		device	180
		NNMi	211
		node groups	208
		Status tab	93
		Interface form	72
		IP Address form	75
		Layer 2 Connection form	108
		Node Component form	44
		Node form	48
		SNMP Agent form	54
		Stream Correlation Incidents view	172
		subnet	
		adding notes	113
		details	114
		naming	113
		routers	112
		view	19
		viewing details	114
		switch	
		connectivity between devices	104
		finding attached port	204
		monitoring	116

---

---

routers	112	Performance	70
Switches map	103	Ports	35, 86
		Registration	50, 55, 73, 111, 114, 148
		Router Redundancy Members	80
		Status	44, 48, 54, 72, 75, 93, 108
		Tracked Objects	83
		Virtual IPAddresses	84
		VLAN Ports	64
		VLANs	87
		tasks	
		assigning incidents	149
		incident view	132
		troubleshooting	13
		telnet	207
		Temperature Sensor is Out of Range incident	196
		testing nodes	206
		threshold	
		incidents	199
		tools menu	177
		Topology Maps workspace	101-103
		Topology Source	21
		traceroute command	117, 206
		track priority	83
		Tracked Objects	
		form	84
		monitoring configuration	178
		tab	83
		tracking	
		incidents	
		progress	157
		traps, SNMP	
		displaying	175
		troubleshooting	
		abnormal network behavior	13
		connectivity problems	104, 112

---

T			
table views			
capabilities added to node object	36		
checking node groups	208		
invoking actions	204		
monitoring	120		
navigating	177, 180, 206-207		
Path View	114		
types	15		
viewing object details	27		
tables, SNMP ipRoute	117		
tabs			
Additional Filters	90, 96		
Additional Nodes	90		
Capabilities	35-36, 66		
Child Node Groups	92		
Component Health	40		
Conclusions	45, 49, 54, 73, 76, 109		
Correlated Children	142		
Correlated Parents	142		
Custom Attributes	39, 69, 142		
Device Filters	89		
Diagnostics	46-47, 147		
General	32, 63, 135		
Health Attribute	42		
IfType Filters	95		
Incidents	44, 48, 55, 71, 75, 85, 108		
Interface Groups	70		
Interfaces	33, 107		
IP Addresses	33, 64, 114		
Link Aggregation	65, 109		
Node Groups	39		

---

## Index: Troubleshooting workspace – views

---

determining problem scopes	129
devices	21
incidents	132, 134-135, 142, 147-148, 172
interface	60, 63-65, 70-73
IP addresses	73, 75-76, 78
network	
alerts	181
problems	120, 177
node groups	208
nodes	28, 32-35, 39-40, 42, 44-50, 192
Troubleshooting workspace	104, 112, 114
trunk ports	86

### U

Unassigned Key Incidents view	163
Unassigned Vital Incidents view	149-150
unassigning incidents	150
unmanageable interface	190
unresponsive	
incident	187
nodes	195
updating	
discovery information	177
incidents	151, 157
lifecycle states	157
node status	180
utilization	
CPU	188
incidents	200

### V

varbind values	143
vendor devices	
defining	58

---

verifying	
device	
configuration details	177
status	180
network health	211
viewing	
incidents	130, 143
interface group	
details	25
managed device details	27
network connectivity maps	98
node details	130
node group	
details	25
views	
Closed Key Incidents	168
Critical Interfaces	120
Critical Nodes	121
Custom Incidents	159, 173
Custom Interfaces	23
Custom IP Addresses	24
Custom Nodes	23
filtering	16, 124
device categories	21
interface types	22
Incidents by Family	173
Interface by Administrative State	125
Interface by IfType	22
Interface Group	25
InterfacePerformance	127
interfaces	17
Interfaces by Operational State	126
Interfaces by Status	125
IP Addresses	19
IP Addresses by State	126

---



IP Subnets	19	Virtual IPAddresses	
Key Incident	160	form	85
Layer 2 Connections	21	tab	84
Layer 2 Neighbors	104	virtual LANs	20, 86
Layer 3 Neighbors	112	Vital Incidents by Lifecycle State view	169
Management Stations	26	VLAN	
My Open Incidents	149, 160	form	86
NNM 6.x/7.x Events	174	view	20
NNM 6.x/7.x Events by Category	174	VLAN Ports tab	
Node Groups	25, 128	Interface form	64
nodes	16	Node form	34
Nodes by Device Category	21	VLANs tab	
Nodes by Status	124	Port form	87
Non-Normal Interfaces	122	Voice-Over-IP	16
Non-Normal Nodes	122	Voltage is Out of Range incident	197
Non-Normal Router Redundancy	123	VRRP	
Not Responding Address	124	nodes	118
Open Key Incidents	161		
Open Key Incidents by Category	166	<b>W</b>	
Open Key Incidents by Family	167	watching status colors	129
Open Key Incidents by Priority	165	workspaces	
Open Key Incidents by Severity	164	Topology Maps	101-103
out-of-box	15, 120, 159		
Root Cause Incidents	170-171		
Router Redundancy Group	24		
SNMP Traps	175		
SNMP Traps by Family	175		
Stream Correlation Incidents	172		
types	15		
Unassigned Key Incidents	163		
Unassigned Vital Incidents	149-150		
updating lifecycle state	157		
Vital Incidents by Lifecycle State	169		
VLANs	20		



