

# HP Network Node Manager i Software

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

Software Version: 9.23

---

[Online Help: Help for Operators](#)

Document Release Date: May 2013

Software Release Date: May 2013



# 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.

### **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 America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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

## Copyright Notice

© Copyright 2008–2013 Hewlett-Packard Development Company, L.P.

## Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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.

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

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

## Acknowledgements

This product includes software developed by the Apache Software Foundation.  
(<http://www.apache.org>)

This product includes software developed by the Indiana University Extreme! Lab.  
(<http://www.extreme.indiana.edu>)

## Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

# Support

Visit the HP Software Support Online web site at:

**<http://www.hp.com/go/hpsoftwaresupport>**

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

**<http://h20229.www2.hp.com/passport-registration.html>**

To find more information about access levels, go to:

**[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)**

## Disclaimer for PDF Version of Online Help

This document is a PDF version of the 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, causing format problems. Some elements of online help are completely removed from the PDF version. Those problem topics can be successfully printed from within the online help.

---

# Contents

Online Help: Help for Operators .....	1
Contents .....	7
Using Network Node Manager .....	19
Node and Incident Access .....	19
Change Your Password .....	20
NNMi's Global Network Management Feature (NNMi Advanced) .....	21
Is the Global Network Management Feature Enabled (NNMi Advanced)? .....	22
View the NNMi Management Servers' Domain List (NNMi Advanced) .....	23
Accessing NNM 6.x and 7.x Features .....	25
Learning Your Network Inventory .....	26
Filter Views by Node or Interface Group .....	26
Nodes View (Inventory) .....	27
Interfaces View (Inventory) .....	29
IP Addresses View (Inventory) .....	30
SNMP Agents View .....	31
IP Subnets View (Inventory) .....	32
VLANs View (Inventory) .....	33
Cards View .....	34
Ports View .....	34
Node Components View .....	35
Layer 2 Connections View (Inventory) .....	35
Nodes by Management Server View (Inventory) .....	36
Nodes (All Attributes) View (Inventory) .....	37
Interfaces (All Attributes) View (Inventory) .....	37
IP Addresses (All Attributes) View (Inventory) .....	39
MIB Variables View .....	39
MIB Notifications View .....	40

MIB Notification Form .....	40
Card Redundancy Groups View (Inventory) .....	42
Router Redundancy Group View (NNMi Advanced) .....	42
Router Redundancy Group Members View (Inventory) (NNMi Advanced) .....	43
Node Groups View (Inventory) .....	44
Interface Group View (Inventory) .....	44
Management Stations View (6.x/7.x) (Inventory) .....	45
MPLS WAN Clouds (RAMS) (NNMi Advanced) .....	46
<b>Accessing Device Details .....</b>	<b>47</b>
Node Form .....	50
Node Form: General Tab .....	59
Node Form: IP Addresses Tab .....	60
Node Form: Interfaces Tab .....	61
Node Form: Cards Tab .....	61
Node Form: Ports Tab .....	61
Node Form: VLAN Ports Tab .....	62
VLAN Port Form .....	62
Node Form: Router Redundancy Group Tab (NNMi Advanced) .....	63
Node Form: Capabilities Tab .....	63
Node Capabilities Provided by NNMi .....	64
Node Capability Form .....	67
Node Form: Custom Attributes Tab .....	68
Node Custom Attributes Form .....	68
Node Form: Node Groups Tab .....	69
Node Form: Node Components Tab .....	69
Node Form: Custom Polled Instances Tab .....	71
Node Form: Diagnostics Tab (NNM iSPI NET) .....	72
Node Diagnostic Results Form (Flow Run Result) (NNM iSPI NET) .....	73
Node Form: Incidents Tab .....	74
Node Form: Status Tab .....	75
Node Form: Conclusions Tab .....	76
Node Form: Registration Tab .....	83



Device Profile Form .....	84
Device Family Form .....	88
Device Vendor Form .....	89
Device Category Form .....	89
Interface Form .....	90
Interface Form: General Tab .....	95
Interface Form: IP Addresses Tab .....	97
Interface Form: Ports Tab .....	97
Interface Form: VLAN Ports Tab .....	97
Interface Form: Link Aggregation Tab (NNMi Advanced) .....	98
Interface Form: Capabilities Tab .....	102
Interface Capabilities Provided by NNMi .....	103
Interface Capability Form .....	110
Interface Form: Custom Attributes Tab .....	111
Interface Custom Attributes Form .....	111
Interface Form: Interface Groups Tab .....	112
Interface Form: Performance Tab (NNM iSPI Performance for Metrics) .....	112
Interface Form: Incidents Tab .....	114
Interface Form: Status Tab .....	115
Interface Form: Conclusions Tab .....	116
Interface Form: Registration Tab .....	131
IP Address Form .....	132
IP Address Form: Incidents Tab .....	134
IP Address Form: Capabilities Tab .....	135
IP Address Capabilities Provided by NNMi .....	135
IP Address Capability Form .....	137
IP Address Form: Status Tab .....	137
IP Address Form: Conclusions Tab .....	138
IP Address Form: Registration Tab .....	139
SNMP Agent Form .....	140
SNMP Agent Form: Status Tab .....	146
SNMP Agent Form: Conclusions Tab .....	147

SNMP Agent Form: Incidents Tab .....	153
SNMP Agent Form: Registration Tab .....	153
IP Subnet Form .....	154
IP Subnet Form: IP Addresses Tab .....	155
IP Subnet Form: Registration Tab .....	155
VLAN Form .....	156
VLAN Form: Ports Tab .....	157
Card Form .....	157
Card Form: General Tab .....	163
Card Form: Ports Tab .....	164
Card Form: Daughter Cards Tab .....	164
Card Form: Capabilities Tab .....	165
Card Capabilities Provided by NNMi .....	165
Card Capability Form .....	166
Card Form: Incidents Tab .....	167
Card Form: Status Tab .....	167
Card Status History Form .....	168
Card Form: Conclusions Tab .....	169
Card Form: Registration Tab .....	170
Port Form .....	171
Port Form: VLANs Tab .....	172
Port Form: Registration Tab .....	173
Node Component Form .....	173
Node Component Form: Monitored Attributes Tab .....	176
Node Component Monitored Attribute Form .....	176
Node Component Form: Incidents Tab .....	179
Node Component Form: Status Tab .....	179
Node Component Form: Conclusions Tab .....	180
Node Component Form: Registration Tab .....	188
Layer 2 Connection Form .....	188
Layer 2 Connection Form: Interfaces Tab .....	191
Layer 2 Connection Form: Incidents Tab .....	191

Layer 2 Connection Form: Status Tab .....	192
Layer 2 Connection Form: Conclusions Tab .....	193
Layer 2 Connection Form: Link Aggregation Tab (NNMi Advanced) .....	199
Layer 2 Connection Form: Registration Tab .....	203
Card Redundancy Group Form .....	204
Card Redundancy Group Form: Redundant Cards Tab .....	205
Card Redundancy Group Form: Incidents Tab .....	205
Card Redundancy Group Form: Status Tab .....	206
Card Redundancy Group Status History Form .....	206
Card Redundancy Group Form: Conclusions Tab .....	207
Router Redundancy Group Form (NNMi Advanced) .....	209
Router Redundancy Group Form: Router Redundancy Members Tab (NNMi Advanced) .....	210
Router Redundancy Member Form (NNMi Advanced) .....	211
Router Redundancy Member Form: Tracked Objects Tab (NNMi Advanced) ..	213
Tracked Objects Form (NNMi Advanced) .....	215
Router Redundancy Group Form: Virtual IP Addresses Tab (NNMi Advanced) .....	216
Virtual IP Addresses Form (NNMi Advanced) .....	216
Router Redundancy Group Form: Incidents Tab (NNMi Advanced) .....	217
Router Redundancy Group Form: Status Tab (NNMi Advanced) .....	217
Router Redundancy Group Status History Form (NNMi Advanced) .....	217
Router Redundancy Group Form: Conclusions Tab (NNMi Advanced) .....	218
Router Redundancy Group Form: Registration Tab (NNMi Advanced) .....	222
Node Group Form .....	223
Node Group Form: Device Filters Tab (NNMi Administrators only) .....	224
Node Device Filter Form (NNMi Administrators only) .....	225
Node Group Form: Additional Filters Tab (NNMi Administrators only) .....	226
Node Group Form: Additional Nodes Tab (NNMi Administrators only) .....	226
Additional Node Form (NNMi Administrators only) .....	227
Node Group Form: Child Node Groups Tab (NNMi Administrators only) .....	228
Node Group Hierarchy (Child Node Group) Form (NNMi Administrators only) .....	229
Node Group Form: Status Tab .....	230

Interface Group Form .....	232
Interface Group Form: ifType Filters Tab .....	233
ifType Filter Form .....	234
ifType (Interface Type) Form .....	234
Interface Group Form: Additional Filters Tab .....	235
MPLS WAN Cloud (RAMS) Form (NNMi Advanced) .....	235
MPLS WAN Cloud (RAMS) Form: MPLS WAN Connections Tab (NNMi Advanced) .....	236
Custom Node Collections Form .....	237
Custom Node Collections Form: Incidents Tab .....	239
Custom Node Collections Form: Status Tab .....	239
Custom Node Collections Form: Conclusions Tab .....	240
Custom Node Collections Form: Polled Instances Tab .....	241
Custom Polled Instance Form .....	242
Custom Polled Instance Form: Incidents Tab .....	245
Custom Polled Instance Form: Status Tab .....	245
Custom Polled Instance Form: Conclusions Tab .....	246
Custom Polled Collection Form .....	247
Comparison Map Form .....	250
<b>Viewing Maps (Network Connectivity) .....</b>	<b>252</b>
Node Group Maps .....	253
Navigating within a Node Group Map .....	256
Position Nodes on a Node Group Map .....	257
Node Group Overview Map .....	257
Initial Discovery Progress or Network Overview Map .....	258
Networking Infrastructure Devices Map .....	259
Routers Map .....	260
Switches Map .....	260
Display the Layer 2 Neighbor View .....	261
Display the Layer 3 Neighbor View .....	263
Path Between Two Nodes that Have IPv4 Addresses .....	265
Path Calculation Rules .....	267
Path View Limitations .....	270

Investigate Errors and Performance Issues .....	271
MPLS WAN Cloud Map (NNMi Advanced) .....	271
Enhanced Path View (NNMi Advanced) .....	272
<b>Monitoring Devices for Problems .....</b>	<b>274</b>
Monitor with Table Views .....	274
Non-Normal Node Components View .....	275
Non-Normal Cards View .....	276
Non-Normal Interfaces View .....	276
Non-Normal Nodes View .....	277
Non-Normal SNMP Agents View .....	279
Not Responding Address View .....	279
Interface Performance View (NNM iSPI Performance for Metrics) .....	280
Card Redundancy Groups View (Monitoring) .....	280
Router Redundancy Group View (NNMi Advanced) .....	281
Node Groups View (Monitoring) .....	282
Custom Node Collections View (Monitoring) .....	282
Custom Polled Instances View .....	282
Monitor with Map Views .....	284
Watch Status Colors .....	285
Determine Problem Scope .....	286
Access a Problem Device .....	287
Access Node Details .....	287
Access All Related Incidents .....	290
Export Maps to Microsoft® Visio (NNM iSPI NET) .....	290
Hide Connections or Connection Labels from an Exported Visio Diagram (NNM iSPI NET) .....	292
View the Details for a Map Object on an Exported Visio Diagram (NNM iSPI NET)	293
Print an Exported Visio Diagram (NNM iSPI NET) .....	293
Monitor with Line Graphs .....	294
Using Line Graphs .....	295
Change the Lines Displayed on a Line Graph .....	295
Emphasize a Line Displayed on a Line Graph .....	297

Hide a Line Displayed on a Line Graph .....	297
Show and Hide the Line Graph Legend .....	298
Change the Polling Interval for a Graph .....	299
Select a Time Segment Using the Timeline Viewer .....	299
Unlock the Y-Axis When Viewing a Time Segment .....	300
Change the Zoom Value for a Graph .....	301
Display Data Values on a Graph .....	301
Display Messages on a Line Graph .....	302
Determine the Maximum Time Range for a Graph .....	303
Print a Graph .....	303
Export Graph Data to a Comma-Separated Values (CSV) File .....	304
Line Graphs Provided by NNMi .....	305
Display a Line Graph from an Incident (Custom Poller Only) .....	306
Display a Line Graph for a Custom Polled Instance .....	307
<b>Monitoring Incidents for Problems .....</b>	<b>309</b>
Organize Your Incidents .....	311
Incident Form .....	311
Incident Form: General Tab .....	314
Incident Form: Correlated Parents Tab .....	320
Incident Form: Correlated Children Tab .....	320
Incident Form: Custom Attributes Tab .....	321
Custom Incident Attribute Form .....	321
Custom Incident Attributes Provided by NNMi (Information for Operators) .....	322
Incident Form: Diagnostics Tab (NNM iSPI NET) .....	328
Incident Diagnostic Results Form (Flow Run Result) (NNM iSPI NET) .....	329
Incident Form: Registration Tab .....	330
Manage Incident Assignments .....	331
Own Incidents .....	331
Assign Incidents .....	332
Unassign Incidents .....	333
Keep Your Incidents Up to Date .....	334
About the Incident Lifecycle .....	335

Track an Incident's Progress .....	336
Display a Map from an Incident .....	337
Island Node Group Map .....	338
Apply an Action to an Incident Source Node or Source Object .....	338
Monitor Incidents in a Global Network Management Environment (NNMi Advanced) .....	340
Incident Views Provided by NNMi .....	340
My Open Incidents View .....	342
Key Incident Views .....	343
Open Key Incidents View .....	344
Unassigned Open Key Incidents View .....	345
Closed Key Incidents View .....	346
Root Cause Incidents .....	347
Open Root Cause Incidents View .....	348
Service Impact Incidents View .....	349
All Incidents View .....	350
Custom Open Incidents View .....	350
Custom Incidents View .....	351
NNM 6.x/7.x Events View .....	352
Syslog Messages View (HP ArcSight) .....	353
SNMP Traps View .....	353
<b>Investigate and Diagnose Problems .....</b>	<b>355</b>
Use the Analysis Pane .....	356
Verify Device Configuration Details .....	359
View the Monitoring Settings Report .....	360
View MIB Information for a Node (MIB Browser) .....	362
MIB Browser Keyboard Navigation .....	363
Determine a Node's Supported MIBs (MIB Browser) .....	363
Display a MIB File's Contents (MIB Browser) .....	365
Determine a Node's MIB Variable Values (MIB Browser) .....	365
Display MIB Variable Details .....	367
MIB Variable Form .....	369
Enumerated Values Form .....	372

Table Indices Form .....	373
Display a MIB Table (MIB Browser) .....	374
Check SNMP Support for a Node (MIB Browser) .....	377
Find an Entry in the MIB Browser Output .....	378
Export MIB Browser Output .....	380
Copy Selected MIB Browser Output (MIB Browser) .....	382
Print MIB Browser Output (MIB Browser) .....	383
Verify Current Status of a Device .....	385
Interpret Root Cause Incidents .....	387
Address Not Responding .....	388
Aggregator Interface Degraded (NNMi Advanced) .....	389
Aggregator Interface Down (NNMi Advanced) .....	390
Aggregator Connection Degraded (NNMi Advanced) .....	391
Aggregator Connection Down (NNMi Advanced) .....	393
Buffer has Insufficient Capacity or is Malfunctioning .....	394
Card Disabled .....	395
Card Down .....	395
Card Undetermined State .....	396
Connection Down .....	397
CPU Utilization is too High .....	398
Custom Polled Instance in Collection is Out of Range .....	399
Fan is Out of Range or Malfunctioning .....	400
Interface Down .....	401
Interface Disabled .....	402
IP Subnet Contains IP with New MAC Address .....	403
Memory has Insufficient Capacity or is Malfunctioning .....	404
Node Down .....	404
Node or Connection Down .....	406
Power Supply is Out of Range or Malfunctioning .....	407
Island Group Down .....	408
SNMP Agent Not Responding .....	409
SNMP Agent Ping Not Responding .....	410



Temperature Sensor is Out of Range .....	411
Voltage is Out of Range .....	411
Interpret Incidents Related to SNMP Traps .....	412
Hosted Object Trap Storm .....	413
Message Queue Incident Rate Exceeded (NNMi Advanced) .....	414
Message Queue Size Exceeded (NNMi Advanced) .....	415
Pipeline Queue Size Exceeded .....	415
SNMP Trap Limit (Warning, Major or Critical) .....	416
Trap Storm .....	417
Interpret Informational Incidents .....	418
Card Removed .....	418
Card Inserted .....	418
Node Deleted .....	419
Interpret Service Impact Incidents .....	419
Multiple Primary Cards in Card Redundancy Group .....	420
Multiple Primary Devices in Router Redundancy Group (NNMi Advanced) .....	421
Multiple Secondary Devices in Router Redundancy Group (NNMi Advanced) .....	421
No Primary Card in Card Redundancy Group .....	422
No Primary Device in Router Redundancy Group (NNMi Advanced) .....	423
No Secondary Card in Card Redundancy Group .....	424
No Secondary Device in Router Redundancy Group (NNMi Advanced) .....	425
Primary Device in Router Redundancy Group Switched (NNMi Advanced) .....	426
Router Redundancy Group Degraded (NNMi Advanced) .....	426
Interpret Threshold Incidents .....	427
Backplane Incidents (NNM iSPI Performance for Metrics) .....	431
Buffer Incidents (NNM iSPI Performance for Metrics) .....	432
CPU Incidents (NNM iSPI Performance for Metrics) .....	433
Disk Incidents (NNM iSPI Performance for Metrics) .....	434
Interface Frame Check Sequence (FCS) Error Rate Incidents (NNM iSPI Performance for Metrics) .....	436
Interface Input and Output Discard Rate Incidents (NNM iSPI Performance for Metrics) .....	437
Interface Input and Output Error Rate Incidents (NNM iSPI Performance for Metrics) .....	439

Input and Output Queue Drop Incidents (NNM iSPI Performance for Metrics) .....	441
Interface Input and Output Utilization Incidents (NNM iSPI Performance for Metrics) .	443
Management Address ICMP Response Time Incidents .....	445
Memory Incidents (NNM iSPI Performance for Metrics) .....	446
Find a Node .....	447
Find the Attached Switch Port .....	449
Display End Nodes Attached to a Switch .....	452
Test Node Access (Ping) .....	454
Find the Route (traceroute) .....	455
Establish Contact with a Node (Telnet or Secure Shell) .....	456
Check Status Details for a Node Group .....	458
Checking the Status of NNMi .....	460
Glossary .....	461

# Chapter 1

---

## 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	"Monitoring Devices for Problems" on page 274 and "Investigate and Diagnose Problems" on page 355
Annotate information for future diagnosis	"Accessing Device Details" on page 47
Look for historical information to proactively monitor the network	"Monitoring Incidents for Problems" on page 309
View an inventory of what is being managed	"Learning Your Network Inventory" on page 26
Change your password	"Change Your Password" on the next page
Check NNMi health	"Checking the Status of NNMi" on page 460

## Node and Incident Access

NNMi enables an NNMi administrator to limit visibility and control to parts of the network for some or all operators. Tenants are the top-level organization to which a node belongs.

Security Groups enable an NNMi administrator to group objects that require the same access level.

Security Group Mapping controls (through User Groups) which User Accounts can access a node and its hosted objects, such as an interface. Each node is associated with only one Security Group and Tenant.

**Note:** Users see only those members of an object group (for example, Node Group or Router Redundancy Group) for which they have access. If a user cannot access any nodes in the group, the group is not visible to that user.

If your NNMi administrator has configured Security Groups to limit node access, then as a network operator you can view a node and its associated incidents only if one of the User Groups to which you belongs is associated with that node's Security Group.

**Note:** If a node is deleted, only an NNMi administrator can view the incidents associated with that node.

**Tip:** Select **Help** → **System Information** to view the User Account, **NNMi Role**<sup>1</sup>, and User Groups for the current NNMi session.

## Change Your Password

**Note:** If your assigned NNMi Role is *Guest*, you cannot change the password. Contact your NNMi administrator to request a change of password.

NNMi administrators can allow certain users to change their NNMi password at any time using **File** → **Change Password**.

To change your NNMi password:

1. Select **File** → **Change Password**.
2. In the **Old Password** attribute, type your current password.
3. In the **New Password** attribute, type your new password.
4. In the **Confirm Password** attribute, retype your new password.
5. Click **OK**.

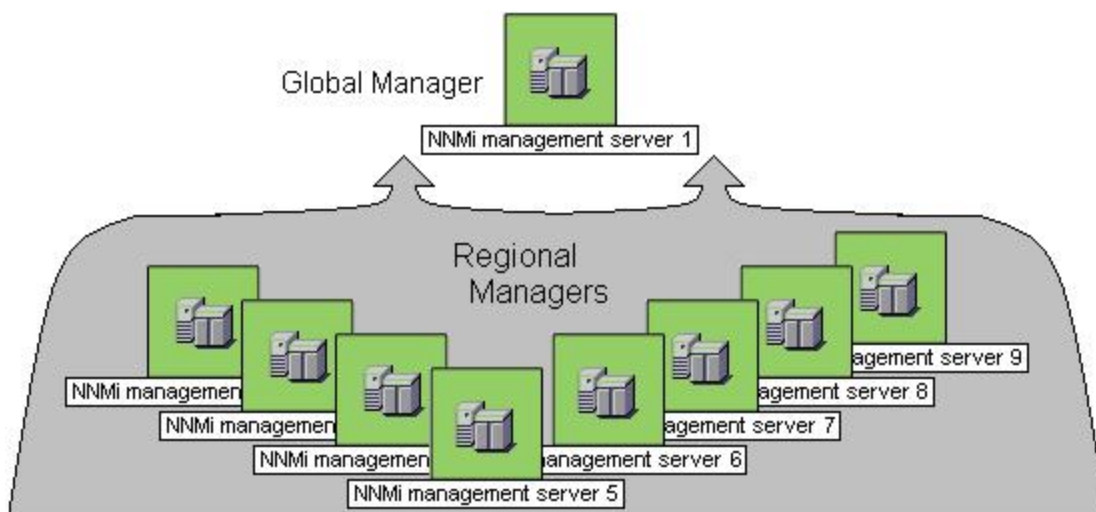
---

<sup>1</sup>Determined by your membership in one of four special NNMi User Groups (NNMi Administrators, NNMi Level 2 Operators, NNMi Level 1 Operators, or NNMi Guest Users). This membership determines what you can see and do within the NNMi console.

## Chapter 2

# NNMi's Global Network Management Feature (*NNMi Advanced*)

(*NNMi Advanced*) The NNMi Global Network Management feature enables multiple NNMi management servers to work together while managing different geographic areas of your network. Each NNMi management server discovers and monitors a portion of the network. Specific NNMi management servers can be designated as Global Manager to display combined Node object data.



(*NNMi Advanced*) There are many benefits to using the NNMi Global Network Management feature:

- Provides safe and secure communication among multiple NNMi management servers.
- Provides a central big-picture view of your corporate-wide network on the Global Manager for 24-hour/7-days-per-week coverage.
- Enables management of nodes that are configured with address translation protocols to provide their public address (resulting in overlapping addresses domains). An NNMi Regional Manager is required for each address domain configured with following protocols:
  - *Static* Network Address Translation (NAT)
  - *Dynamic* Network Address Translation (NAT)
  - *Dynamic* Port Address Translation (PAT/NAPT)
- Easy to set up:
  - Each Regional Manager administrator specifies *all Node object data* or *a specific Node Group* for participation at the Global Manager level.
  - Each Global Manager administrator specifies which Regional Managers are permitted to contribute information.

- Automatically combines topology from multiple NNMi management servers on the Global Manager, but keeps management responsibilities separate. (No duplication, the responsible NNMi Management server is clearly identified per Node.)
- Generates and manages Incidents independently on each server (generated within the context of topology available on each server).
- Regional Manager administrators can configure specific SNMP traps or NNM 6.x/7.x Events to be forwarded from Regional Managers to Global Managers.

*(NNMi Advanced - Global Network Management feature)* The Global Manager and the Regional Manager maintain separate sets of data. Conclusions about each Node are derived from the available data and can sometimes be different. Regional Managers forward the results of each Spiral Discovery cycle to the Global Manager. The Regional Manager can have a Node Group filter configured to limit the amount of data that is forwarded to the Global Manager. Filters are usually unnecessary for Global Network Management. Do not filter out nodes that are important for connectivity in your network environment to ensure NNMi has the data needed for accurate root cause analysis.

- The Global Manager might know information about why a connection from one site to another is down, but the Regional Manager just knows that the router connected to that remote site has an interface that is down. Use **Actions** → **Regional Manager Console** to see the other perspective.
- When troubleshooting a Node on the Global Manager, you can use **Actions** → **Open from Regional Manager** to see the latest Node information on the Regional Manager.

After Global Network Management is set up in your network environment:

- To determine if your NNMi management server is a Global Manager or a Regional Manager, see ["Is the Global Network Management Feature Enabled \(NNMi Advanced\)?"](#) below.
- To determine which Nodes are monitored by each NNMi management server, see ["View the NNMi Management Servers' Domain List \(NNMi Advanced\)"](#) on the next page.
- To determine which Incidents were forwarded to the Global Manager, see ["Monitor Incidents in a Global Network Management Environment \(NNMi Advanced\)"](#) on page 340 .

## Is the Global Network Management Feature Enabled (*NNMi Advanced*)?

*(NNMi Advanced)* The NNMi Global Network Management feature enables multiple NNMi management servers to work together while managing different geographic areas of your network. See ["NNMi's Global Network Management Feature \(NNMi Advanced\)"](#) on the previous page for more information.

- Is your NNMi management server a Global Manager that displays information from other NNMi management servers (Regional Managers)? Click here to find out:
  - a. Open the NNMi console.
  - b. Select **Help** → **System Information**.
  - c. Do you see a **Global Network Management** tab?

- d. If yes, on the **Global Network Management** tab, do you see a **Regional Managers Reporting to this Global Manager** section?
  - If yes, this NNMi management server is functioning as a Global Manager.
  - If no, this NNMi management server is not a Global Manager.

The NNMi administrators in your network environment determine which NNMi management server functions as a Global Manager.

- Is your NNMi management server a Regional Manager that contributes data to one or more Global Managers? Click here to find out:
  - a. Open the NNMi console.
  - b. Select **Help** → **System Information**.
  - c. Do you see a **Global Network Management** tab?
  - d. If yes, in the **Global Network Management** tab, do you see the **Reporting to Global Managers** section?
    - If yes, this NNMi management server is functioning as a Regional Manager.
    - If no, this NNMi management server is not a Regional Manager.

To make this NNMi management server a Regional Manager, the NNMi administrator for some other NNMi management server must create a Global Network Management connection to this NNMi management server.

## View the NNMi Management Servers' Domain List (*NNMi Advanced*)

*(NNMi Advanced - Global Network Management feature)* If your NNMi management server is a Global Manager, you can see network information from multiple NNMi management servers. You can easily determine which list of nodes each NNMi management server is discovering and monitoring.

**To display the list of nodes assigned to each NNMi management server, use one of the following methods:**

Navigate to the **Nodes by Management Server** view.

1. Open the NNMi console on the Global Manager (NNMi management server).
2. From the workspace navigation panel, select the **Inventory** workspace.
3. Select the **Nodes by Management Server** view.
4. Click the drop-down filter in the view to display a list of all NNMi management servers in your Global Network Management environment.

Local = The NNMi management server you are currently signed into.

<name> = The name your NNMi administrator assigned to a Regional Manager (NNMi management server). If you see a <name> value, it means that you are currently signed into a Global Manager, and other NNMi management servers report to this NNMi management server.

See ["Nodes by Management Server View \(Inventory\)" on page 36](#) for more information about this view.

Navigate to the **Nodes** view.

1. Open the NNMi console on the Global Manager (NNMi management server).
2. From the workspace navigation panel, select the **Inventory** workspace.
3. Select the **Nodes** view.
4. At the far right of the view, click the **NNMi Management Server** column heading to sort the view by the responsible NNMi management server's name:

Local = The NNMi management server you are currently signed into.

<name> = The name your NNMi administrator assigned to a Regional Manager (NNMi management server). If you see a <name> value, it means that you are currently signed into a Global Manager, and other NNMi management servers report to this NNMi management server.

5. Scroll up or down through the rows in this view to locate the entire list of devices being managed by each NNMi management server.

See ["Nodes View \(Inventory\)" on page 27](#) for more information about this view.



# Chapter 3

---

## 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 (6.x/7.x)** 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 \(6.x/7.x\) \(Inventory\)](#)" on page 45 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 use 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**

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

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.

## Chapter 4


---

# Learning Your Network Inventory

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

Within any table view, you can quickly view a few additional properties of your network devices. To do so, click the row representing a network object. NNMi provides Analysis Pane information at a glance for 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, double-click the row that contains the object information. The form containing the information for the object's attributes appears.

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 list 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 Views by Node or Interface Group](#)" below 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](#).

The **Views with Inventory Lists** section in [Views Provided by NNMi](#) provides a short description of each Inventory view.

## 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 can 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 an Interface Group.

Node Group filters are available for:

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

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

Interface Group filters are available for:

- Interface views
- IP Address views
- Card views
- Node Component views

**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, **Interfaces**.
2. In the  group selector drop-down list, select the Node Group or Interface Group you want to use as a filter.

When using Node Group or Interface Group filters, note the following:

- By default, table views are not filtered by Node or Interface Group.
- If a view can be filtered by both Node Group and Interface Group, the selection box lists the Node Groups first, followed by the Interface Groups. Each list appears in alphabetical order.
- When the filter is applied, the view automatically refreshes to show the appropriate set of objects.
- If you set a Node Group or Interface Group filter, NNMi combines the group filter with any other filters using the AND Boolean operator.
- To clear the group filter, return the selection value to "<Set node group filter>" or "<Set node or interface group filter>".

## Nodes View (Inventory)

**Tip:** See "Node Form" on page 50 for more details about the node attributes that appear in this view's column headings.

The Nodes view 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, whether the SNMP agent is enabled or not, date indicating the last time the node status was modified, which NNMi management server is responsible for this node, and any notes included for the node.

**To display the Nodes view:**

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **Nodes** view.

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.
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 in 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.
<p><i>(NNMi Advanced - Global Network Management feature)</i> If your NNMi management server is a Global Manager, identify which nodes are managed by each Regional Manager.</p>	<p>See "<a href="#">NNMi's Global Network Management Feature (NNMi Advanced)</a>" on page 21 for more information. Sort the Node view using the NNMi Management Server column (at the far right of the view).</p> <p>Local = The NNMi management server you are currently signed into.</p> <p>&lt;name&gt; = The name your NNMi administrator assigned to a Regional Manager (NNMi management server). If you see a &lt;name&gt; value, it means that you are currently signed into a Global Manager, and other NNMi management servers report to this NNMi management server.</p>

#### Related Topics:

[Using Table Views](#)

["Node Form" on page 50](#)

Export Table Information

## Interfaces View (Inventory)

**Tip:** See "Interface Form" on page 90 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.

### To display the Interfaces view:

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **Interfaces** view.

If you see several blank columns for an interface in a table view, note the following:

- The interface might be in a non-SNMP node.

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**.

**Note:** For **Pseudo Interface**, NNMi attempts to obtain additional information using a variety of *discovery protocols* (see the list of Topology Source protocols in [Layer 2 Connection Form](#)).

- 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.
- The interface might be a Nortel private interface.  
For Nortel SNMP interfaces, note the following:
  - The interface index (`ifIndex`) value is set according to the Nortel private MIB.
  - NNMi tries to collect the MAC address and interface name using Nortel's private MIBs.
- (*NNMi Advanced*) The interface might be an IPv-6 interface.  
A small number of IPv6 devices do not support the standard RFC 2863 IF-MIB for IPv6 interfaces. In this case, NNMi uses the *RFC 2465 IPv6-MIB*. When this happens, note the following:
  - Interface index (`ifIndex`) and description (`ifDescr`) are set according to the RFC 2465 IPv6 MIB.

- Interface type (`ifType`) is set to `Other` (no specific type is available).
- Interface Name (`ifName`), Alias (`ifAlias`), and Speed (`ifSpeed`) are blank (not available).
- NNMi monitors the Status of this interface, but Performance metrics are not available.

When an IP Address has the Interface Name (`ifName`) attribute set to blank, NNMi constructs an alternate string for the IP Address's **In Interface** attribute (`Other [<ifIndex_value>]`).

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.
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="#">"Filter Views by Node or Interface Group" on page 26</a> for more information.

#### Related Topics:

[Using Table Views](#)

["Interface Form" on page 90](#)

[Export Table Information](#)

## IP Addresses View (Inventory)

**Tip:** See ["IP Address Form" on page 132](#) for more information about the IP address attributes that appear in this view's column headings.

The IP Addresses view 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.

**To display the IP Addresses view:**

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **IP Addresses** view.

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="#">Filter Views by Node or Interface Group</a> " on page 26 for more information.

#### Related Topics:

[Use Table Views](#)

["IP Address Form" on page 132](#)

[Export Table Information](#)

## SNMP Agents View

**Tip:** See "[SNMP Agent Form](#)" on page 140 for more details about the SNMP Agent attributes that appear in this view's column headings.

The **Non-Normal SNMP Agents** view in the **Monitoring** workspace is useful for identifying all of the SNMP Agents that have a state that is other than Normal.

#### To display the Non-Normal Node SNMP Agents view:

1. In the **Workspaces** navigation pane, select the **Monitoring** workspace.
2. Select the **Non-Normal SNMP Agents** view.

For each SNMP Agent displayed in the view, you can identify the SNMP Agent Status, the Agent SNMP State, the Agent ICMP State, the Management Address ICMP Response Time, the Management Address ICMP Response Time Baseline, the associated node Name value (**Hosted**

**On Node**, the IP address NNMi uses to communicate with this SNMP agent (Management Address), the date and time the Status was last modified, the version of the SNMP protocol in use, whether the SNMP agent is set up for SNMP communication in the network environment (Agent Enabled), the User Datagram Protocol port configuration for this SNMP agent (UDP Port), the time that NNMi waits for a response to an SNMP query before reissuing the request, and the maximum number of retries that NNMi issues for an SNMP query before determining the query result to be "unresponsive", the SNMP Proxy address, and the SNMP Proxy port.

**Note:** If you have Administrator Role, the SNMP Agents view also displays the Read Community String.

### Related Topics

[Use Table Views](#)

[Export Table Information](#)

## IP Subnets View (Inventory)

**Tip:** See "IP Subnet Form" on page 154 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.

### To display the IP Subnets view:

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **IP Subnets** view.

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 154](#)

[Export 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. After the VLAN is established, the participating devices behave "as if" they were all connected to one LAN. For example, switches within the same layer 2 switching fabric (switches that hear one another and do not have layer 3 routers between them) can be in a VLAN (identified by the *VLAN Identifier* value, the VLAN Id).

Several VLANs can co-exist within a network. Devices can participate in multiple VLANs. And trunk ports 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.

VLANs that reside in separate broadcast domains *can have identical names*. And one VLAN can have multiple names. For example, two switches participate in the same VLAN (*VLAN Id=10*), but the VLAN name is different on each switch. Those switches are nonetheless still participating in the same VLAN.

**Tip:** To sort the VLANs view and group all devices in a particular VLAN together, click the *VLAN Id* column heading.

### 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 because that is the default VLAN Identifier, but NNMi discovers any higher numbered VLANs.

3. Use the VLAN view to quickly identify all of the switch port VLANs configured in your network environment:

The table displays a row for each VLAN member and columns for the following:

- Global VLAN Name  
VLAN connections are determined by a common VLAN Id. The *name* assigned to that VLAN can be designated by each participating Node's configuration settings for that VLAN Id. Therefore, NNMi chooses a VLAN name for this value (from potentially many names for the same VLAN ID). NNMi uses the lowest sort-order name from all available names designated by member Nodes.
- VLAN Id (identifier value)
- Member Node Count
- Member Node[Interface] (`hostname[Interface Name]`)

**Tip:** 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 156](#)

[Export Table Information](#)

## Cards View

**Tip:** See ["Card Form" on page 157](#) for more details about the Card attributes that appear in this view's column headings.

The Card view is useful for identifying all of the Cards hosted on the nodes that are stored in the NNMi database. To view the Cards per node, sort the Card view by the **Hosted On Node** attribute.

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

### To display the Cards view:

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **Cards** view.

For each Card displayed in this view, you can identify the Card Status, Administrative State, Operational State, Name of the Node in which the card resides (Hosted On Node), the date and time the Status was last modified, the Card Name, model, Type (hardware-type designator), Serial Number, Firmware Version, Software Version, Index, Physical Index, Hosted on Card (name of the card, if any, in which the selected card is attached), Redundant Group, if any, in which the card participates, and a Description, and any Notes for the Card.

### To see the incidents related to a Card:

1. Double-click the row representing a Card. The ["Card Form" on page 157](#) displays all details about the selected Card.
2. Navigate to the **Incidents** tab to see the incidents associated with the selected Card.

### Related Topics

[Use Table Views](#)

[Export Table Information](#)

## Ports View

**Tip:** See ["Port Form" on page 171](#) for more details about the Port attributes that appear in this view's column headings.

The Ports view is useful for identifying all of the Ports hosted on the nodes that are stored in the NNMi database. To view the Ports per node, sort the Ports view by the **Hosted On Node** attribute.

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

### To display the Ports view:

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **Ports** view.

For each Port displayed in this view, you can identify the name of the Node in which the Card resides (Hosted On Node), the Port Name, index number, Type (hardware-type designator), Speed, Configured Duplex Setting, if any, the Card on which the Port resides, and the interface to which the Port is associated.

### **Related Topics**

[Use Table Views](#)

[Export Table Information](#)

## **Node Components View**

**Tip:** See "Node Component Form" on page 173 for more details about the Node Component attributes that appear in this view's column headings.

The Node Components view is useful for identifying all of the Node Components that NNMi monitors on the nodes including the following:

- Fan
- Power Supply
- Temperature
- Voltage

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

### **To display the Node Components view:**

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **Node Components** view.

For each Node Component displayed in this view, you can identify the Node Component Status, Name, type (for example Fan), the associated hostname (Hosted On Node), and the date and time the Status was last modified.

### **Related Topics**

[Use Table Views](#)

[Export Table Information](#)

## **Layer 2 Connections View (Inventory)**

**Tip:** See "Layer 2 Connection Form" on page 188 for more details about the Layer 2 Connection attributes that appear in this view's column headings.

The Layer 2 Connections view 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.

**To display the Layer 2 Connections view:**

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **Layer 2 Connections** view.

**Related Topics**

[Export Table Information](#)

## Nodes by Management Server View (Inventory)

**Tip:** See "Node Form" on page 50 for more details about the node attributes that appear in this view's column headings.

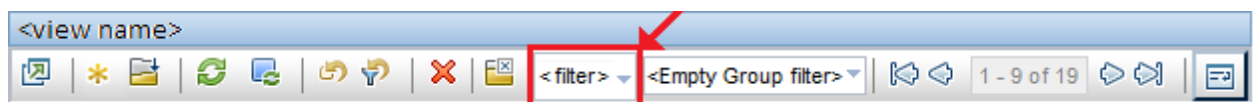
(*NNMi Advanced*) The Global Network Management feature enables multiple NNMi management servers to share the workload in your network environment. See "NNMi's Global Network Management Feature (NNMi Advanced)" on page 21 for more information about this feature.

If the Global Network Management feature is enabled in your environment, and your NNMi management server is a Global Manager, the **Nodes by Management Server** view provides a filter to show which nodes each NNMi management server is responsible for discovering and monitoring:

Local = The NNMi management server you are currently signed into.

<name> = The name your NNMi administrator assigned to a Regional Manager (NNMi management server). If you see a <name> value, it means that you are currently signed into a Global Manager, and other NNMi management servers report to this NNMi management server.

**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:



**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.

**To display the Nodes by Management Server view:**

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **Nodes by Management Server** view.
3. Click the filter drop-down and choose the name of the NNMi management server that has the list of Nodes you want to view.

For each node displayed, you can identify its overall status (for example, **Normal**, **Warning**, **Minor**, **Major**, **Critical**, or **Unknown**), device category, 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](#)

[Export Table Information](#)

## Nodes (All Attributes) View (Inventory)

**Tip:** See "Node Form" on page 50 for more details about the node attributes that appear in this view's column headings.

The Nodes (All Attributes) 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.

**To display the Nodes (All Attributes) view:**

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **Nodes (All Attributes)** view.

The Nodes (All Attributes) 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, whether the SNMP agent is enabled, the 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, which NNMi management server is responsible for this node, the system object ID (MIB-II sysObjectID), the device vendor, the device family, the name of its SNMP agent, the SNMP protocol version, the Agent SNMP state, the Agent ICMP state, the date the node's state was last modified, the Tenant and Security Group assigned to the node, its [discovery state](#), time of the last discovery cycle, the creation date, and the date and time the node was last modified.

See "Nodes View (Inventory)" on page 27 for more information about ways to use a node view.

**Related Topics:**

[Use Table Views](#)

[Export Table Information](#)

## Interfaces (All Attributes) View (Inventory)

**Tip:** See "Interface Form" on page 90 for more details about the interface attributes that appear in this view's column headings.

The **Interfaces (All Attributes)** 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 status, its administrative state 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.

**To display the Interfaces (All Attributes) view:**

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **Interfaces (All Attributes)** view.

If you see several blank columns for an interface in a table view, note the following:

- The interface might be in a non-SNMP node.

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**.

**Note:** For **Pseudo Interface**, NNMi attempts to obtain additional information using a variety of *discovery protocols* (see the list of Topology Source protocols in [Layer 2 Connection Form](#)).

- 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.
- The interface might be a Nortel private interface.  
For Nortel SNMP interfaces, note the following:
  - The interface index (`ifIndex`) value is set according to the Nortel private MIB.
  - NNMi tries to collect the MAC address and interface name using Nortel's private MIBs.
- (*NNMi Advanced*) The interface might be an IPv-6 interface.  
A small number of IPv6 devices do not support the standard RFC 2863 IF-MIB for IPv6 interfaces. In this case, NNMi uses the *RFC 2465 IPv6-MIB*. When this happens, note the following:
  - Interface index (`ifIndex`) and description (`ifDescr`) are set according to the RFC 2465 IPv6 MIB.
  - Interface type (`ifType`) is set to `Other` (no specific type is available).
  - Interface Name (`ifName`), Alias (`ifAlias`), and Speed (`ifSpeed`) are blank (not available).
  - NNMi monitors the Status of this interface, but Performance metrics are not available.

When an IP Address has the Interface Name (`ifName`) attribute set to blank, NNMi constructs an alternate string for the IP Address's **In Interface** attribute (`Other [<ifIndex_value>]`).

**Related Topics:**

[Use Table Views](#)

[Filter a Table View](#)

[Export Table Information](#)

## IP Addresses (All Attributes) View (Inventory)

**Tip:** See "IP Address Form" on page 132 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.

**To display the IP Addresses (All Attributes) view:**

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **IP Addresses (All Attributes)** 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.

**Related Topics**

[Use Table Views](#)

[Export Table Information](#)

## MIB Variables View

**Tip:** See "MIB Variable Form" on page 369 for more details about the MIB Variable attributes that appear in this view's column headings.

The MIB Variables view displays all of the MIB variables currently available in NNMi.

**Note:** Your NNMi administrator might choose to load additional MIBs. Check this view periodically to view the latest list of MIB variables available.

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

**To display the MIB Variables view:**

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **MIB Variables** view.

For each MIB variable displayed in this view, you can identify the MIB variable's numeric OID (Object Identifier), Name, Syntax and textual OID.

#### **Related Topics**

[Use Table Views](#)

[Export Table Information](#)

## **MIB Notifications View**

**Tip:** See "MIB Notification Form" below for more details about the MIB Notification attributes that appear in this view's column headings.

The MIB Notifications view displays the SNMP trap information that is defined by the associated MIB.

**Note:** Your NNMi administrator might choose to load additional MIBs. Check this view periodically to view the latest list of MIB Notifications available.

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

#### **To display the MIB Notifications view:**

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **MIB Notifications** view.

For each MIB Notification displayed in this view, you can identify the MIB variable's numeric OID (Object Identifier), Name, MIB, and textual OID, as well as the Type, Severity, Category, and State information for the SNMP trap.

#### **Related Topics**

[Use Table Views](#)

[Export Table Information](#)

## **MIB Notification Form**

The MIB Notification form enables you to view the SNMP trap information, if any, that is defined by the selected MIB.

**Note:** If you are an Administrator, you can also access the MIB Notification form from the **Loaded MIBs** option in the **Configuration** workspace. See [MIB Notification Form \(for Administrators\)](#) for more information.

#### **For information about each tab:**

**To view the MIB Notification information for a selected MIB:**



1. From the workspace navigation panel, select the **Inventory** workspace.
2. Select **MIB Notifications**.
3. Double-click the row of interest.
4. View the Basics information for the selected MIB Notification (see the [MIB Notification Basic Attributes](#) table).

### MIB Notification Basic Attributes

Attribute	Description
Name	<p>The Name value that is stored in the MIB definition for the selected MIB notification. In the following example, <code>linkDown</code> is the Name of the MIB variable :</p> <pre>linkDown NOTIFICATION-TYPE OBJECTS { ifIndex, ifAdminStatus, ifOperStatus } STATUS current DESCRIPTION "A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus." ::= { snmpTraps 3 }</pre>
OID (Numeric)	The numeric representation of the OID (Object Identification) value for the selected MIB notification.
OID (Text)	The textual representation of the OID for the selected MIB variable.
MIB	<p>The name value that is stored at the beginning of the MIB definitions to identify the MIB. In the following example, <code>IF-MIB</code> is the name of the MIB:</p> <pre>IF-MIB DEFINITIONS ::= BEGIN</pre>
Description	SNMP Trap Description that is stored in the MIB.
Type	<i>Optional.</i> SNMP Trap <code>--#TYPE</code> value that is stored in the MIB.
Summary	<i>Optional.</i> The <code>--#SUMMARY</code> value that is stored in the MIB for the SNMP Trap.
Arguments	<i>Optional.</i> Number of arguments for the SNMP Trap.
Severity	<i>Optional.</i> The <code>--#SEVERITY</code> value that is stored in the MIB for the SNMP Trap.
Generic	<i>Optional.</i> The <code>--#GENERIC</code> value that is stored in the MIB for the SNMP Trap.
Category	<i>Optional.</i> The <code>--#CATEGORY</code> value that is stored in the MIB for the SNMP Trap.
Source ID	<i>Optional.</i> The <code>--#SOURCE ID</code> value that is stored in the MIB for the SNMP Trap.
State	<i>Optional.</i> The <code>--#STATE</code> value that is stored in the MIB for the SNMP Trap.

## Card Redundancy Groups View (Inventory)

**Tip:** See "Card Redundancy Group Form" on page 204 for more details about the attributes that appear in this view's column headings.

The Card Redundancy Groups view is useful for identifying the names of the groups that provide redundancy protection against card failure.

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

### To display the Card Redundancy Groups view:

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **Card Redundancy Groups View** view.

For each Card Redundancy Group displayed in this view, you can identify the Card Redundancy Group Status, Name, and the date and time the Status was last modified.

### To see the incidents related to a Card Redundancy Group:

1. Double-click the row representing a Card Redundancy Group. The "Card Redundancy Group Form" on page 204 displays all details about the selected Card Redundancy Group.
2. Navigate to the **Incidents** tab to see the incidents associated with the selected Card Redundancy Group.

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

1. Double-click the row representing a Card Redundancy Group. The "Card Redundancy Group Form" on page 204 displays all details about the selected Card Redundancy Group.
2. Navigate to the **Redundant Cards** tab.

Each Card that belongs to the selected Card Redundancy Group is listed.

### Related Topics

[Use Table Views](#)

[Export Table Information](#)

## Router Redundancy Group View (NNMi Advanced)

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.

**Tip:** See "Router Redundancy Group Form (NNMi Advanced)" on page 209 for more details about the Router Redundancy Group attributes that appear in this view's column headings.

### To display the Router Redundancy Group view:

1. In the **Workspaces** navigation pane, select the **Inventory** workspace or the **Monitoring** workspace.
2. Select the **Router Redundancy Group** view.

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. Double-click the row representing a Router Redundancy Group. The "[Router Redundancy Group Form \(NNMi Advanced\)](#)" on [page 209](#) displays all details about the selected Router Redundancy Group.
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:**

1. Double-click the row representing the Router Redundancy Group members you want to see.
2. Navigate to the **Router Redundancy Members** tab.

Each node that belongs to the selected Router Redundancy Group is listed. You also see which interface is assigned to the Router Redundancy Group within each node.

**Related Topics**

[Use Table Views](#)

[Export Table Information](#)

## Router Redundancy Group Members View (Inventory) (NNMi Advanced)

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 Members view to see all of the members of a group of redundant routers in your network.

**Tip:** See "[Router Redundancy Member Form \(NNMi Advanced\)](#)" on [page 211](#) for more details about the Router Redundancy Group Member attributes that appear in this view's column headings.

**To display the Router Redundancy Group Member view:**

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **Router Redundancy Group Members** view.

For each Router Redundancy Group Member displayed in the view, you can identify the Router Redundancy Group Member [Current State](#), its Previous State, the Router Redundancy Group Name, the hostname on which the Router Redundancy Group Member resides, the interface that is being used by the router to participate in the Router Redundancy Group (Redundancy Interface), the IP Address used to exchange the configured Router Redundancy Protocol messages between routers in the Router Redundancy Group (Primary IP), the number used to rank the Router Redundancy Members (Priority), the date and time the Router Redundancy Member State was last

modified, and whether the Router Redundancy Group Member owns the Virtual IP Address for the Router Redundancy Group (for example, [VRRP](#)<sup>1</sup> protocol).

### Related Topics

[Use Table Views](#)

[Export Table Information](#)

## Node Groups View (Inventory)

**Tip:** See "Node Group Form" on page 223 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 can 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 Views by Node or Interface Group" on page 26 for more information about filtering views using node groups.

**Note:** Your NNMi administrator can remove the Nodes Group view from the NNMi console. If you are an NNMi administrator, see the "NNMi Console" chapter of the *HP Network Node Manager i Software Deployment Reference* for more information.

### 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, double-click the row representing a Node Group. The "Node Group Form" on page 223 displays all details about the selected Node Group.

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

[Export Table Information](#)

## Interface Group View (Inventory)

**Tip:** See "Interface Group Form" on page 232 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 can group sets of interfaces into interface

---

<sup>1</sup>Virtual Router Redundancy Protocol

groups. See [About Node and Interface Groups](#) for more information about how your administrator sets up interface groups. See "[Filter Views by Node or Interface Group](#)" on page 26 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, double-click the row representing an Interface Group. The "[Interface Form](#)" on page 90 displays all details about the selected Interfaced Group.

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**

[Export Table Information](#)

## Management Stations View (6.x/7.x) (Inventory)

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

The **Management Stations (6.x/7.x)** view 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 directly accessing the NNM 6.x/7.x management station.

**Note:** 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: Home Base, ovw, Launcher, and Alarms. See "[Accessing NNM 6.x and 7.x Features](#)" on page 25 for more information.

**To view attribute information for any NNM 6.x or 7.x management stations that have been configured:**

1. In the **Workspaces** navigation pane, select the **Inventory** workspace.
2. Select the **Management Stations (6.x/7.x)** view.

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

**Related Topics**

[Export Table Information](#)

## MPLS WAN Clouds (RAMS) (*NNMi Advanced*)

**Tip:** See [MPLS WAN Cloud \(RAMS\) form](#) for more details about the attributes that appear in this view's column headings.

*NNMi Advanced.* The MPLS WAN Connections view provides information about the Layer 3 connectivity between your network and any MPLS networks (for example, an Internet Service Provider MPLS network).

**Note:** Each MPLS network is represented in the associated topology map by an MPLS WAN Cloud.

Information displayed in the MPLS WAN Clouds (RAMS) view includes the name and Autonomous System Number assigned to the MPLS Cloud as well as the number of Customer Edge (CE) routers associated with the MPLS WAN Cloud.

### Related Topics:

[Use Table Views](#)

[Export Table Information](#)

# Chapter 5

---

## 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 an Analysis Pane that displays related information about an object. NNMi performs the appropriate analysis on the object and determines the related information to display. See ["Use the Analysis Pane "](#) on page 356 for more information.

### **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** workspace, **Nodes** view).
3. Double-click the row representing an 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 50
  - ["SNMP Agent Form"](#) on page 140
  - ["Interface Form"](#) on page 90
  - ["IP Address Form"](#) on page 132
  - ["SNMP Agent Form"](#) on page 140
  - ["IP Subnet Form"](#) on page 154
  - ["VLAN Form"](#) on page 156
  - ["Card Form"](#) on page 157
  - ["Port Form"](#) on page 171
  - ["Node Component Form"](#) on page 173
  - ["Layer 2 Connection Form"](#) on page 188
  - ["MIB Variable Form"](#) on page 369
  - ["MIB Notification Form"](#) on page 40
  - ["Card Redundancy Group Form"](#) on page 204
  - ["Router Redundancy Group Form \(NNMi Advanced\)"](#) on page 209
  - ["Router Redundancy Member Form \(NNMi Advanced\)"](#) on page 211

- "Node Group Form" on page 223
- "Interface Group Form" on page 232

**Tip:** A form is also available for incidents, see "Incident Form" on page 311.


**Note:** The SNMP Agent form is also accessed from the Node form. The Port form is also accessed from the VLAN form.

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


1. Display a map using the **Topology Maps** or **Troubleshooting** workspace, or the **Actions** → menu.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.


**Note:** If the map requires a starting node before it displays, enter the name or IP Address for the starting node you want to use.

2. After the map displays, 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.

**To access the Analysis Pane from a table view:**

1. Select the workspace of interest (for example,  **Inventory**).
2. Select the view that contains the object of interest (for example, the **Nodes** view).
3. Select the row that contains the object of interest.
4. NNMi displays detailed information at the bottom of the view in the Analysis Pane.


**To access the Analysis Pane in a map view:**


1. Select the workspace of interest (for example,  **Topology Maps**).
2. Select a map view (for example, select **Routers**).

**Note:** If the map requires a starting node before it opens, enter the name or IP Address for the starting node you want to use.

3. Click the map object of interest.
4. NNMi displays detailed information at the bottom of the view in the Analysis Pane.

**To access the Analysis Pane in a form:**

- Click the form's toolbar  Show Analysis icon to display information about the current form's top-level object in the Analysis Pane.

**Note:**  Show Analysis always displays the top-level object's information.

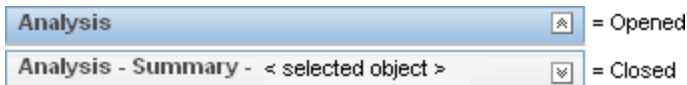
- Click a row in a table on one of the form's tabs to display detailed information about the selected object in the Analysis Pane.



NNMi displays detailed information at the bottom of the form in the Analysis Pane. See [Working with Objects](#) for more information about forms.

Note the following:

- Look for one of the following at the bottom of the display area:



Open the Analysis Pane if necessary by clicking the expand button.

- Place your mouse cursor over the title bar to display the symbol, then resize as necessary.
- The Analysis Pane remains blank until an object is selected.
- If you select multiple objects or clear a selection, NNMi retains the Analysis Pane's contents.
- If you change views, NNMi clears the Analysis Pane.
- Click any Refresh icon in the Analysis Pane to update a subset of displayed information.
- NNMi automatically refreshes the entire Analysis Pane's contents when you save a form.
- The Gauges tab shows real-time SNMP gauges to display State Poller and Custom Poller SNMP data.
  - These gauges are displayed for Nodes, Interfaces, Custom Node Collections, and for Node Components of type CPU, Memory, Buffers, or Backplane.
  - NNMi displays a gauge for each significant MIB Object Identifier (OID) that the node or interface supports, up to the default maximum of 24.

**Tip:** If you are an NNMi administrator, for information about using the `nms-ui.properties` file to change this default, see the "NNMi Console" chapter in the *HP Network Node Manager i Software Deployment Reference*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>.

- Each gauge displays the current OID value, using the default refresh rate of 15 seconds. (If you are an NNMi administrator, for information about using the `nms-ui.properties` file to change this default, see the "NNMi Console" chapter of the *HP Network Node Manager i Software Deployment Reference*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>.)
- The value range displayed indicates the OID minimum and maximum values that NNMi has encountered.
- For any gauge that tracks percentage values, NNMi uses a red line to indicate where the OID value is near 100 percent.
- There is not a one-to-one match between the OIDs used to analyze monitoring thresholds and those displayed in the Analysis Pane. For example, the Analysis Pane might display a **Cisco Memory Pool** OID value that does not match the value used to calculate whether the **Memory Utilization** Monitored Attribute threshold is reached or exceeded. This is because some threshold metrics require more complex calculations than a single OID allows.

**Tip:** If a gauge label appears to be a duplicate value, mouse over the label to view the more complete tooltip name that appears. (If you are an NNMi administrator, to change the gauge title from the NNMi component name to the SNMP MIB variable name, see the "Maintaining NNMi" chapter of the *HP Network Node Manager i Software Deployment Reference*, which is available at:

<http://h20230.www2.hp.com/selfsolve/manuals.>)

- To launch an SNMP Line Graph for the selected metric, click the icon that appears at the bottom of each gauge.
- To select and copy the tooltip information, double-click the gauge. NNMi opens a text window that enables you to select and copy the tooltip information.

**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 [ports](#), the [VLAN ports](#), the [SUMP agent](#), the [device profile](#), and the [incidents](#) associated with this node.

If your role permits, 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 dynamically generated name assigned to this device.</p> <p>The NNMi administrator configures how NNMi populates this attribute through two configuration settings: (1) The <b>Node Name Resolution</b> attributes in Discovery Configuration (full or short DNS name, full or short sysName, IP address). (2) The Name <i>might be</i> converted to all uppercase or all lowercase (depending on how the NNMi administrator configured settings in the <code>nms-topology.properties</code> file). See the "Modifying NNMi Normalization Properties" section of the <i>HP Network Node Manager i Software Deployment Reference</i>, which is available at: <a href="http://h20230.www2.hp.com/selfsolve/manuals.">http://h20230.www2.hp.com/selfsolve/manuals.</a></p> <p>This name is used in table views and maps.</p>
Hostname	<p>The fully-qualified hostname currently stored in the NNMi database for this device (according to any hostname resolution strategy currently in use in your network environment; for example, DNS).</p>

## Basic Attributes, continued

Attribute	Description
	<p>NNMi follows a set of rules to dynamically generate the value stored in the NNMi database for each Node's Hostname. Click here for details.</p> <ul style="list-style-type: none"><li>• If the Node supports SNMP, NNMi requests the Hostname using the IP Address of the associated SNMP agent (the Management Address attribute value on the Node form).</li></ul> <p>When the NNMi administrator chooses <b>Enable SNMP Address Rediscovery</b> <input checked="" type="checkbox"/> in the Communication Configuration:</p> <ul style="list-style-type: none"><li>▪ If the SNMP Agent does not respond, NNMi checks for another Management Address to request the Hostname, and the Hostname could change.</li><li>▪ If the SNMP Agent associated with the node changes, the Management Address and Hostname could change.</li></ul> <p>When the NNMi administrator disables <b>Enable SNMP Address Rediscovery</b> <input type="checkbox"/> in the Communication Configuration:</p> <ul style="list-style-type: none"><li>▪ If the SNMP Agent does not respond, NNMi uses the previously gathered Management Address attribute value to request the Hostname.</li><li>▪ If the SNMP Agent associated with the node changes, NNMi uses the previously gathered Management Address attribute value to request the Hostname.</li></ul> <ul style="list-style-type: none"><li>• If the Node does not support SNMP, no Management Address is available. NNMi requests a Hostname starting with the lowest IP Address associated with the node (a Discovery Seed value or an IP address value gathered from a neighboring device). NNMi uses the first Hostname provided. The Hostname might change during a future discovery cycle.</li></ul> <p><b>Note:</b> NNMi administrators can use NNMi property file settings to change the way NNMi determines Hostname values:</p> <ul style="list-style-type: none"><li>• <code>nms-topology.properties</code> file settings: If DNS is the source of the Node's Hostname, there are three choices. By default NNMi uses the exact Hostname from your network configuration. It is possible to change NNMi behavior to convert Hostnames to all uppercase or all lowercase. See the "Modifying NNMi Normalization Properties" section of the <i>HP Network Node Manager i Software Deployment Reference</i>, which is available at: <a href="http://h20230.www2.hp.com/selfsolve/manuals">http://h20230.www2.hp.com/selfsolve/manuals</a>.</li><li>• <code>nms-disco.properties</code> file settings: The Hostname is either requested from the Node's lowest loopback interface IP address that resolves to a Hostname or requested from the Node's designated Management Address (SNMP agent address). With either choice, when no IP address resolves to a Hostname, the IP address itself becomes the Hostname. See the "Maintaining NNMi"</li></ul>

## Basic Attributes, continued

Attribute	Description
	<p>chapter of the <i>HP Network Node Manager i Software Deployment Reference</i>, which is available at:  <a href="http://h20230.www2.hp.com/selfsolve/manuals">http://h20230.www2.hp.com/selfsolve/manuals</a>.</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> <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 first discovers a node, the <i>seed address</i> (provided by the NNMi administrator) or discovered address (for non-seeded nodes) becomes the initial Management Address of the node. After NNMi builds an inventory of all IP addresses associated with the node, NNMi follows a set of rules to determine which address is the best choice as the node's Management Address. Click here for details.</p> <p><b>Note:</b> With NNMi Advanced, the NNMi administrator specifies whether NNMi prefers IPv4 or IPv6 addresses when selecting the Management Address. See <a href="#">Configure Default SNMP, Management Address, and ICMP Settings</a>.</p> <ol style="list-style-type: none"> <li>1. NNMi ignores the following addresses when determining which Management Address is most appropriate: <ul style="list-style-type: none"> <li>■ Any address of an administratively-down interface.</li> <li>■ Any address that is virtual (for example, <a href="#">VRRP</a><sup>1</sup>).</li> <li>■ Any IPv4 <a href="#">Anycast Rendezvous Point IP Address</a><sup>2</sup> or IPv6 Anycast address.</li> <li>■ Any address in the reserved loopback network range. IPv4 uses 127/24 (127.*.*.*) and IPv6 uses ::1.</li> <li>■ Any <a href="#">IPv6 link-local address</a><sup>3</sup>.</li> </ul> </li> <li>2. If the NNMi Administrator specifies Enable SNMP Address Rediscovery in</li> </ol>

<sup>1</sup>Virtual Router Redundancy Protocol

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

<sup>3</sup>A non-routable IPv6 unicast address only used for communication with other nodes on the same link (LAN or VLAN). Link local addresses cannot be used for communication that must be forwarded through a router. IPv6 auto-configuration automatically assigns a unique link local address in the fe80::/10 address space to each IPv6-enabled interface on a system.




## Basic Attributes, continued

Attribute	Description
	<p>Communication Configuration, NNMi prefers the last-known Management Address (if any).</p> <p>3. If the Management Address does not respond and the NNMi Administrator specifies Enable SNMP Address Rediscovery in Communication Configuration, NNMi uses the Communication Configuration settings for <i>Management Address Selection</i>. The NNMi Administrator chooses the order in which NNMi checks the following:</p> <ul style="list-style-type: none"><li>■ Seed IP / Management IP - If the NNMi Administrator configures a Seed, NNMi uses the Seed address (either a specified IP address or the DNS address associated with a specified hostname) only during initial Discovery. NNMi then requests the current Management Address (the address from which the node's SNMP Agent responds) and uses that IP address for all communication after initial discovery.</li><li>■ Lowest Loopback - If a node supports multiple <b>loopback address</b><sup>1</sup>, NNMi queries each loopback addresses, starting with the lowest number. NNMi uses the loopback address with the lowest number from which the SNMP agent responds (for example, 10.16.42.197 is a lower number than 10.16.197.42).</li><li>■ Highest Loopback - If a node supports multiple <b>loopback address</b><sup>2</sup>, NNMi queries each loopback addresses, starting with the highest number. NNMi uses the loopback address with the highest number from which the SNMP agent responds.</li><li>■ Interface Matching - The NNMi Administrator chooses which interface MIB variable NNMi queries to detect changes. NNMi can use the following MIB-II attribute values: <code>ifIndex</code>, <code>ifName</code>, <code>ifDescr</code>, <code>ifAlias</code>, or a combination of these (<code>ifName</code> or <code>ifDescr</code>, <code>ifName</code> or <code>ifDescr</code> or <code>ifAlias</code>).</li></ul> <p>4. If no response, NNMi queries any remaining IP addresses in the node's IP address inventory, starting with the lowest number. NNMi uses the address with the lowest number from which the SNMP agent responds.</p> <p>5. If no response, NNMi checks for any Mapped Address configured for one of the currently known addresses (see the Mapped Address column in the</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 Number 24, softwareloopback from the IANA ifType-MIB.

<sup>2</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 Number 24, softwareloopback from the IANA ifType-MIB.





### Basic Attributes, continued

Attribute	Description
	<p>Custom IP Addresses view).</p> <p><b>Note:</b> The address represents a <i>static</i> Network Address Translation (NAT) pair's <i>external IP address</i> from the internal/external IP address pair. NNMi Administrators configure these pairs using the Overlapping IP Address Mapping form. NNMi uses this list of addresses starting with IPv4 from low to high, then IPv6 from low to high.</p> <ol style="list-style-type: none"> <li>If no response, NNMi might be configured to repeat the sequence using SNMPv1, SNMPv2c, or SNMPv3 in the order specified by the NNMi administrator (Communication Configurations <i>SNMP Minimum Security Level</i> settings).</li> <li>When all else fails, NNMi retains the last known Management Address (if any) and automatically changes the State of that SNMP Agent object to Critical.</li> </ol> <p>This process is repeated during each Spiral Discovery cycle, and the Management Address can change. For example, NNMi's inventory of addresses for the node expands, or the current Management Address does not respond to SNMP queries due to network problems or node reconfiguration. The NNMi administrator can prevent changes to the management address using the Communication Configurations <i>Enable SNMP Address Rediscovery</i> or <i>Preferred Management Address</i> setting.</p> <p>If this field shows unexpected results:</p> <ul style="list-style-type: none"> <li>Use the <b>Actions</b> → <b>Polling</b> → <b>Configuration Poll</b> command to gather the most current information about this node.</li> </ul> <p><b>Tip:</b> You can right-click any object in a table or map view to access the <b>Actions</b> menu.</p> <ul style="list-style-type: none"> <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>
Status	<p>Overall status for the current node. NNMi follows the ISO standard for status classification. See the "<a href="#">Node Form: Status Tab</a>" on page 75 for more information. Possible values are:</p> <ul style="list-style-type: none"> <li> No Status</li> <li> Normal</li> <li> Disabled</li> </ul>

### Basic Attributes, continued

Attribute	Description
	<p>  Unknown   Warning   Minor   Major   Critical         </p> <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</a> tab. Status reflects the most serious outstanding conclusion. See "<a href="#">Watch Status Colors</a>" on page 285 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> <p>  <b>Managed</b> – Indicates the node is managed by NNMi.   <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.   <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.         </p> <p>This attribute is useful for notifying NNMi when a device has been temporarily out of service, or should never be managed.</p> <p><i>(NNMi Advanced - Global Network Management feature)</i> Any change to the Node's Management Mode setting is immediately sent from a Regional Manager (NNMi management server) to the Global Manager. (Changes to Management Mode for other objects are sent during the next Spiral Discovery cycle on the Regional Manager.)</p> <p><b>Note:</b> If the NNMi Security configuration permits, you can change this setting using <b>Actions</b> → <b>Management Mode</b>. To change the Management Mode back to <b>Managed</b> for the selected Node object and change the Management Mode back to <b>Managed</b> or <b>Inherited</b> for all associated interfaces and addresses, use the <b>Actions</b> → <b>Management Mode</b> → <b>Managed (Reset All)</b>.</p>
Device Profile	Name of the device profile that determines how devices of this type are managed and the icon and background shape displayed on maps.

**Basic Attributes, continued**












Attribute	Description
	<p>Click the  Lookup icon and select  Open to display the "Device Profile Form" on page 84 for more information.</p>
<p>Tenant</p>	<p>Tenants enable NNMi administrators to partition a network across multiple customers.</p> <p>A Tenant is the top-level organization to which a Node belongs.</p> <p>NNMi administrators can use this drop-down to change the Tenant assignment for a Node, or use the  Lookup icon and select  New to create a new Tenant. Use caution when changing the Tenant assignment, see <a href="#">Change Tenant Assignment for a Node</a>.</p> <p>Devices that belong to the Default Tenant can have Layer 2 Connections to any device in any Tenant. Devices within any Tenant <i>other than</i> Default Tenant can have Layer 2 Connections <i>only</i> to devices within the same Tenant or the Default Tenant.</p>
<p>Security Group</p>	<p>Security Group Mappings specify which User Groups have access a node. NNMi users see only those nodes assigned to their Security Group Mapping. You see a node and its associated incidents only if one of the User Groups to which you belong is mapped to that node's Security Group.</p> <p>NNMi administrators assign each node to a Security Group. Each node is associated with only one Security Group. An NNMi administrator can use this attribute to change the Security Group for a node.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> This attribute displays after the NNMi administrator defines more than one Security Group.</p> </div>
<p>NNMi Management Server</p>	<p><i>(NNMi Advanced)</i> This attribute only appears if the Global Network Management feature is enabled and you are using a Global Manager. See "<a href="#">NNMi's Global Network Management Feature (NNMi Advanced)</a>" on page 21 for more information.</p> <p>Local = The NNMi management server you are currently signed into.</p> <p>&lt;name&gt; = The name your NNMi administrator assigned to a Regional Manager (NNMi management server). If you see a &lt;name&gt; value, it means that you are currently signed into a Global Manager, and other NNMi management servers report to this NNMi management server.</p>

**SNMP Agent State Attributes**






Attribute	Description
<p>Agent Enabled</p>	<p>Indicates whether this SNMP agent is set up for SNMP communication in your network environment.</p>
<p>Agent</p>	<p>Indicates whether the SNMP Agent assigned to this node is available and how</p>





**SNMP Agent State Attributes, continued**

Attribute	Description
SNMP State	<p>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 responds to SNMP queries.</li> <li> <b>Not Responding</b> – Indicates that the SNMP agent does not respond to SNMP queries.</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. The SNMP Agent's address might or might not have an associated polling policy.</li> <li> <b>No Polling Policy</b>– Indicates that this SNMP Agent's address is being polled, but no polling policy exists in any Monitoring Configuration settings for this monitored attribute.</li> <li> <b>Unset</b> – Currently not used by NNMi.</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>
Management Address ICMP State	<p>Indicates whether NNMi is communicating with the management address. Possible values are:</p> <ul style="list-style-type: none"> <li> <b>Responding</b> – Indicates that the management address is being polled and is responding to an ICMP ping.</li> <li> <b>Not Responding</b> – Indicates that the management address is being polled, but is not responding to an ICMP ping.</li> </ul> <p>The following values indicate NNMi encountered trouble while trying to gather the required data:</p> <ul style="list-style-type: none"> <li> <b>No Polling Policy</b> - No polling policy exists in Monitoring Configuration settings for this monitored attribute.</li> <li> <b>Not Polled</b> - Indicates that this attribute is intentionally not polled, based on current Monitoring Configuration settings, current Communication Configuration settings, current polling policies, or because the parent Node is set to Not Managed or Out of Service.</li> <li> <b>Unavailable</b> - Unable to determine the State. For example, the ICMP poll returned a value outside the range of possible values or returned a null value.</li> <li> <b>Unset</b> – Currently not used by NNMi.</li> </ul> <p><b>Note:</b> NNMi's State Poller determines the State. The current state</p>

**SNMP Agent State Attributes, continued**

Attribute	Description
	<p>contributes towards the status calculation for the SNMP Agent.</p> <p>See the "SNMP Agent Form: Status Tab" on page 146 tab for more information.</p>
<p>Management Address ICMP Response Time</p>	<p><b>Tip:</b> This attribute is not visible unless the NNMi administrator enables ICMP communication between NNMi and this node.</p> <p>NEW ON NODE FORM [does this attribute only appear if they purchased the iSPI? Or does NNMi do this polling independent of the iSPI?:  <i>(HP Network Node Manager iSPI Performance for Metrics Software)</i> The ICMP response time between the NNMi management server and the selected node. Possible values are:</p> <p> <b>Abnormal Range</b> – Indicates response time (in milliseconds) is outside the normal range when compared to the baseline data collected for this Management Address.</p> <p> <b>Normal Range</b> - Indicates response time (in milliseconds) is normal when compared to the baseline data collected for this Mmanagement Address.</p> <p>OLD:</p> <p><b>Note: Enable Management Address ICMP Polling</b> must be selected. See "Interface Form: Performance Tab (NNM iSPI Performance for Metrics)" on page 112 for more information.</p> <p>Indicates the State of the ICMP response time between the management server and the selected node. Possible values are:</p> <p> <b>Unavailable</b> - Unable to determine the State. For example, the ICMP poll returned a value outside the range of possible values or returned a null value.</p> <p> <b>Nominal</b> - Indicates the ICMP response time was between 0 and the configured High Value.</p> <p> <b>High</b> - Indicates a higher than configured ICMP response time between the management server and the selected node.</p>
<p>Management Address ICMP Response Time Baseline</p>	<p>HP Network Node Manager iSPI Performance for Metrics Software only.</p> <p><b>Note: Enable Node Component Performance Polling</b> must be selected. See "Interface Form: Performance Tab (NNM iSPI Performance for Metrics)" on page 112 for more information.</p> <p>Indicates the ICMP response time between the management server and the selected node is abnormal based on the computed baseline. Possible values are:</p>

### SNMP Agent State Attributes, continued

Attribute	Description
	<p> <b>Abnormal Range</b> – Indicates State Poller has collected values outside the normal range when compared to the baseline data collected for the management address response time.</p> <p> <b>Normal Range</b> - Indicates State Poller collected values within the normal range when compared to the baseline data collected for the management address response time.</p>
State Last Modified	The date and time when the State value was last modified.
Notes	<p><i>(NNMi Advanced - Global Network Management feature)</i> The text you enter here is not sent from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager can add notes that are stored in the NNMi database on the Global Manager.</p> <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, spaces, and special characters (~ ! @ # \$ % ^ &amp; * ( ) _ + -) are permitted.</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 50 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>

### SNMP Values, continued

Attribute	Description
	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.
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 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.
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 Description	Optional MIB-II sysDescr value for the device description. This attribute is set by the device administrator.
SNMP Agent	Name used to identify the SNMP agent. This name is the hostname of the node (as stored in the NNMi database). NNMi chooses the hostname of the parent node according to the criteria specified by your NNMi administrator (see <a href="#">Hostname attribute</a> information).  Click the  ▾ Lookup icon and select  Open to display the "SNMP Agent Form" on page 140 for more information.

### Discovery Attribute

Attribute	Description
Discovery State	Current discovery status for the node. Possible values are:  <b>Newly Created</b> – Indicates the node's hostname and associated IP addresses are in the NNMi database, but NNMi needs to collect more information before determining state, status, and connectivity to other devices in your network environment.  <b>Discovery Completed</b> – Indicates that NNMi collected all of the required information about the node.  <b>Rediscovery in Process</b> – Indicates NNMi is updating information about the node.
Last Completed	Time of the last discovery cycle.

## Node Form: IP Addresses Tab

The "Node Form" on page 50 provides details about the selected node.

*NNMi Advanced*. This table could include all associated IPv4 addresses and IPv6 addresses.

**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>Double-click the row representing an IP address. The "IP Address Form" on page 132 displays all details about the selected IP address.</p>

## Node Form: Interfaces Tab

The "Node Form" on page 50 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>Double-click the row representing an interface. The "Interface Form" on page 90 displays all details about the selected interface.</p>

## Node Form: Cards Tab

The "Node Form" on page 50 provides details about the selected node.

**For information about each tab:**

### Cards Table

Attribute	Description
Cards	<p>Table view of all of the cards associated with the current node.</p> <p>Double-click the row representing a Card. The "Card Form" on page 157 displays all details about the selected Card.</p>

## Node Form: Ports Tab

The "Node Form" on page 50 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 selected node. Use this table to

**Ports Table, continued**

Attribute	Description
	<p>access information about each port associated with the selected node.</p> <p>Double-click the row representing a port. The "Port Form" on page 171 displays all details about the selected port.</p>

## Node Form: VLAN Ports Tab

The "Node Form" on page 50 provides details about the selected node.

**For information about each tab:**

(*NNMi Advanced - Global Network Management feature*) There might be slight differences between the VLAN information shown on Regional Managers and Global Managers, because the VLAN calculations use [Layer 2 Connections](#) data.




**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>Double-click the row representing a VLAN port. The "VLAN Port Form" below displays all details about the selected 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
Local VLAN Name	<p>VLAN connections are determined by a common VLAN Id. The <i>name</i> assigned to that VLAN can be designated by each participating Node/Interface's configuration settings for that VLAN Id.</p> <p>Local VLAN Name = the VLAN name assigned by the configuration settings on the currently selected Node/Interface.</p> <p><b>Tip:</b> If you see an attribute named <i>Global VLAN name</i> = NNMi uses the lowest sort-order name from all available names designated by member Nodes assigned to that VLAN.</p>
VLAN Id	<p>The identification value for the current VLAN. This value is taken directly from the MIB file provided by the Vendor.</p> <p>Click the  Lookup icon and select  Show Analysis or  Open to display more information about the VLAN.</p>

### Basic Attributes, continued

Attribute	Description
Port Name	The port name consists of <Card-number / Port-number>.  Click the  Lookup icon and select  Show Analysis or  Open to display more information about the VLAN.

#### Related Topics:

"Node Form" on page 50

"Interface Form" on page 90

"VLAN Form" on page 156

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

The "Node Form" on page 50 provides details about the selected node.

#### For information about each tab:

##### Router Redundancy Table

Attribute	Description
Router Redundancy	Table view of all of the Router Redundancy Groups associated with the current Node. Use this table to determine all Router Redundancy Groups to which the current Node belongs.  Double-click the row representing a Router Redundancy Group. The "Router Redundancy Group Form (NNMi Advanced)" on page 209 displays all details about the selected Router Redundancy Group.

## Node Form: Capabilities Tab

The "Node Form" on page 50 provides details about the selected node.

#### For information about each 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**<sup>1</sup> group.

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

---

<sup>1</sup>Hot Standby Router Protocol

(*NNMi Advanced - Global Network Management feature*) Any Capability values added by an NNM iSPI are available on the Global Manager only if that iSPI is also running on the Global Manager.

### Capabilities Table

Attribute	Description
Capability	<p>Table of all of the capabilities associated with the selected Node. Use this table to access information about each Capability.</p> <p>Double-click the row representing a Node Capability to open the "Node Capability Form" on page 67 and view more information.</p> <p>For more information, see "Node Capabilities Provided by NNMi" below.</p>

## Node Capabilities Provided by NNMi

The "Node Form: Capabilities Tab" on the previous page displays a table of any Capabilities added to a particular node object. Capabilities enable NNMi and application programmers to provide more information about a node than what is initially stored in the NNMi database. For more information, click any of the following:

- [Basic Node Capability Attribute Values](#)
- [Node Component Capability Attribute Values that are assigned to Nodes \(\\*\)](#)  
These Node Capabilities assist in determining Node Component metrics. See "Node Form: Node Components Tab" on page 69 for more information about health metrics.
- [Card Capability Attribute Values that are assigned to Nodes \(\\*\)](#)
- [NNMi Advanced: Router Redundancy Protocol Capability Attribute Values](#)
- [NNMi Advanced: VMware ESX/ESXi Host and Virtual Machine Capability Attribute Values](#)

External applications can also add Capabilities.

The CISCO-STACK-MIB is associated with multiple Capabilities because NNMi uses the CISCO-STACK-MIB for both card and metrics data.

**KEY:** `com.hp.<product>.capability.<content>.<vendor/org>.<MIB/feature>`

Any Capability provided by NNMi begins with the prefix `com.hp.nnm.capability`.

`<product>` = Either NNMi or the NNM iSPI providing this capability.

`<content>` = card, ipaddr (address), iface (interface), lag ([Link Aggregation](#)<sup>1</sup> interface), node, rp (Router Redundancy), or metric (Node Sensor, Component Health, Component and Device Metrics).

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.



<vendor/org> = Standards organization or vendor defining the MIB or feature associated with the capability.

<MIB/feature> = What this capability measures.

**Note:** The following tables show a few examples of the Capabilities provided by NNMI.

**Basic Node Capability Attribute Values**

Unique Key	Capability	Description
com.hp.nnm.capability.node.ipforwarding	IP Forwarding (Layer 3)	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 "Device Profile Form" on page 84).
com.hp.nnm.capability.node.lanswitching	LAN Switching (Layer 2)	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 "Device Profile Form" on page 84).

**Node Component Capability Attribute Values that are assigned to Nodes**

Unique Key	Capability	Description
com.hp.nnm.capability.rams.node.ramsmplswan cenode	MPLS WAN CE N ode	(NNMI Advanced) The node

**Node Component Capability Attribute Values that are assigned to Nodes, continued**

Unique Key	Capability	Description
		supports HP Router Analytics Management System (RAMS) and MPLS WAN.

**Card Capability Attribute Values that are assigned to Nodes**

Unique Key	Capability	Description
com.hp.nnm.capability.card.ietf.entity	IETF Entity	NNMi discovers but cannot monitor using the Internet Engineering Task Force (IETF) ENTITY-MIB.
com.hp.nnm.capability.card.ietf.entitystate	IETF Entity State	The node supports card monitoring using the Internet Engineering Task Force (IETF) ENTITY-STATE-MIB.

**NNMi Advanced: Router Redundancy Protocol Capability Attribute Values**

Unique Key	Capability	Description
com.hp.nnm.capability.rrp.vrrp	VRRP	<i>NNMi Advanced.</i> The node is a member of a Virtual Router Redundancy Protocol (VRRP)group.

**NNMi Advanced: VMware ESX/ESXi Host and Virtual Machine Capability Attribute Values**

Unique Key	Capability	Description
com.hp.nnm.capability.node.VM	Virtual Machine	<i>NNMi Advanced.</i> The node is a virtual machine being hosted

**NNMi Advanced: VMware ESX/ESXi Host and Virtual Machine Capability Attribute Values, continued**

Unique Key	Capability	Description
		on a VMware ESX/ESXi server. Nodes with this capability become a member of the Node Group named Virtual Machines.
com.hp.nnm.capability.node.hypervisor.vmware.ESX	VMware ESX Host	<i>NNMi Advanced.</i> A VMware ESX/ESXi server that is hosting virtual machines. Nodes with this capability become a member of the Node Group named VMware ESX Hosts.

## 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**<sup>1</sup> group.

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

(*NNMi Advanced - Global Network Management feature*) Any Capability values added by an NNM iSPI are available on the Global Manager only if that iSPI is also running on the Global Manager.

---

<sup>1</sup>Hot Standby Router Protocol

## Node Capability Attributes

Attribute	Description
Capability	Label used to identify the Capability that was added to the node object.  "Node Form: Capabilities Tab" on page 63 shows a list of all available Capabilities for that node.  For more information, see "Node Capabilities Provided by NNMi" on page 64.
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> .  For more information, see "Node Capabilities Provided by NNMi" on page 64.

## 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 permits, you can edit a Custom Attribute. Only users assigned to the NNMi Administrator role can add a Custom Attribute.

### For information about each tab:

(*NNMi Advanced - Global Network Management feature*) Custom Attribute values are not sent from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager can configure Custom Attribute values that are stored in the NNMi database on the Global Manager.

### 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> . For more information, see "Node Custom Attributes Form" below.

## 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.

(*NNMi Advanced - Global Network Management feature*) Custom Attribute values are not sent from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager can configure Custom Attribute values that are stored in the NNMi database on the Global Manager.

### 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> . For more information, see " <a href="#">Node Form: Custom Attributes Tab</a> " on the previous page.

## Node Form: Node Groups Tab

The "Node Form" on page 50 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. Double-click the row representing a Node Group. The " <a href="#">Node Group Form</a> " on page 223 displays all details about the selected Node Group.

## Node Form: Node Components Tab

The "Node Form" on page 50 provides details about the selected node.

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

- Fan
- Power Supply
- Temperature
- Voltage
- Management Address ICMP Response Time

Threshold based on elapsed time (in milliseconds) for receiving a node's reply to an Internet Control Message Protocol (ICMP) echo request. The address queried is the node's Management Address attribute value. See the node's [Node form, Basic Attributes section](#) for the currently configured address.

(*NNM iSPI Performance for Metrics*) If the HP Network Node Manager iSPI Performance for Metrics Software software is installed and configured within your environment, the NNMi administrator can configure threshold for the following performance metrics:

- **Backplane Utilization**  
Threshold based on the percentage of backplane usage compared to the total amount of available backplane resources.
- **Buffer Failure Rate**  
Threshold based on the percentage of a node's buffer failures compared to the total number of attempts to create new buffers. These failures are caused by insufficient memory when the device tried to create new buffers.
- **Buffer Miss Rate**  
Threshold based on the percentage of a Node's buffer misses compared to the total attempts at buffer access. Crossing this threshold indicates the number of available buffers are dropping below a minimum level required for successful operation.
- **Buffer Utilization**  
Threshold based on the percentage of a Node's buffers that are currently in use, compared to the total number of available buffers.
- **CPU 5Sec Utilization**  
Threshold based on the percentage of a node's CPU usage compared to the total amount of available CPU capacity. This percentage is the average CPU utilization over the prior 5-seconds.
- **CPU 1Min Utilization**  
Threshold based on the percentage of a node's CPU usage compared to the total amount of available CPU capacity. This percentage is the average CPU utilization over the prior 1-minute.
- **CPU 5Min Utilization**  
Threshold based on the percentage of a node's CPU usage compared to the total amount of available CPU capacity. This percentage is the average CPU utilization over the prior 5-minutes.
- **Disk Space Utilization**  
Threshold based on the percentage of a node's disk space usage compared to the total amount of available disk space.
- **Memory Utilization**  
Threshold based on the percentage of a node's memory usage compared to the total amount of available memory.

**For information about each tab:**

**Node Components Table**

Attribute	Description
Node Components	<p>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 Node Component metric associated with the selected node.</p> <p>Double-click the row representing a Node Component. The "<a href="#">Node Component Form</a>" on page 173 displays all details about the selected Node Component.</p>









## Node Form: Custom Polled Instances Tab

**Tip:** The "Custom Polled Instance Form" on page 242 provides details about the selected Polled Instance.

**For information about each tab:**

(*NNMi Advanced - Global Network Management feature*) Any Custom Polled Instances are not sent from a Regional Manager (NNMi management server) to the Global Manager. From the Global Manager, use **Actions** → **Open from Regional Manager** to see the list of Custom Polled Instances on the Regional Manager.

**Basics Attributes**

Attribute	Description
Node	Name of the topology node from which the Custom Poller Policy information is being collected. This is the current value in the NNMi database for the Name attribute of the node. The value could be a DNS name, a MIB-II sysName, or an address (depending on how your NNMi administrator configured the discovery process).
State	<p>The State of the Custom Polled Instance as determined by any Thresholds (<a href="#">High State</a> / <a href="#">Low State</a> value) or Comparison Maps (State Mapping = the NNMi administrator assigns a State value for each possible Polled Instance value) configured for the current Custom Poller Collection's MIB Expression.</p> <p>Possible State values for a <i>Polled Instance</i> (Threshold = High State/Low State; or Comparison Map = State Mapping) 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><b>Note:</b> The most severe Threshold <a href="#">High State</a> or <a href="#">Low State</a> value or Comparison Map <i>State Mapping</i> value returned from the Polled Instances for a <a href="#">Custom Node Collection</a> becomes the Custom Node Collection Status.</p>
MIB Variable	<p>Represents the MIB Expression that NNMi polls according to configuration settings. Additional information associated with the MIB Variable includes the MIB Expression Name and any Threshold settings configured for the Custom Poller Collection.</p> <p>Click the  Lookup icon and select  Show Analysis or  Open to display more information about the MIB Variable.</p> <p>See "<a href="#">MIB Variable Form</a>" on page 369 for more information about the MIB Variable attribute.</p>

### Basics Attributes, continued

Attribute	Description
MIB Instance	This attribute contains the multiple filtered instances for the MIB Expression. Each instance value identifies a row in the MIB table.  <b>Note:</b> If a MIB Expression includes multiple MIB Variables that have multiple instances, each instance value that is valid across all MIB Variables for a node is listed here. If NNMi is unable to find the same instance for all MIB Variables in the expression, a Polled Instance is not created. This is because NNMi cannot correctly evaluate a MIB Expression with missing values. If Polled Instances are not created as expected, check the Custom Node Collection view for Discovery State and Discovery State Information values.
Last State Change Value	The value from the MIB Expression that caused the State to change.  <b>Note:</b> A value of <b>null</b> indicates that a value was unavailable or an error occurred while evaluating the MIB Expression.
State Last Modified	The date and time the Polled Instance was last modified.

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

(*HP Network Node Manager iSPI Network Engineering Toolset Software*) The "Node Form" on page 50 provides details about the selected node.

When you access the Node Form: Diagnostics Tab, you can view the history of all the HP Network Node Manager iSPI Network Engineering Toolset Software 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 (iSPI NET only)**.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

### For information about each tab:

(*NNMi Advanced - Global Network Management feature*) Any NNM iSPI Diagnostics Flows are not sent from a Regional Manager (NNMi management server) to the Global Manager. From the Global Manager, use **Actions** → **Open from Regional Manager** to see the list of NNM iSPI Diagnostics Flows on the Regional Manager.

### Diagnostics Table

Attribute	Description
Node Diagnostic Results	Table view of the Node Diagnostic Results associated with the selected node. You can use this table to determine the start time, definition, status, report name, and last update time for each Node Diagnostic Result associated with the selected node.



### Diagnostics Table, continued

Attribute	Description
	Double-click the row representing a Node Diagnostic Result . The "Node Diagnostic Results Form (Flow Run Result) (NNM iSPI NET )" below displays all details about the selected Node Diagnostic Result.

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

HP Network Node Manager iSPI Network Engineering Toolset Software automatically prepares diagnostic reports about the source node when certain incidents are generated and when using **Actions** → **Run Diagnostics (iSPI NET only)**. This form shows details about the currently selected diagnostic report instance.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

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

(*NNMi Advanced - Global Network Management feature*) Any NNM iSPI Diagnostics Flows are not sent from a Regional Manager (NNMi management server) to the Global Manager. From the Global Manager, use **Actions** → **Open from Regional Manager** to see the list of NNM iSPI Diagnostics Flows on the Regional Manager.

See "Node Form: Diagnostics Tab (NNM iSPI NET)" on the previous page for more information.

### 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. Possible values include: <ul style="list-style-type: none"><li>• The Diagnostic is in the queue, but is not yet running</li><li>• The Diagnostic has been submitted and is not finished running</li><li>• The Diagnostic has finished running</li><li>• An error condition prevented the Diagnostic from being submitted</li><li>• NNMi was unable to submit or run the Diagnostic due to a timeout error. The timeout limit for submitting a Diagnostic is one hour. The timeout limit for running a Diagnostic is four hours.</li></ul>

**Diagnostics Table, continued**

Attribute	Description
	<p><b>Tip:</b> 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. NNM iSPI NET uses this text string to display the selected instance of the diagnostics report in a browser window.</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>
Lifecycle State	<p>Incident <a href="#">Lifecycle State</a> of the target Incident.</p> <p>If the incident's Lifecycle State matches the value specified here, the Diagnostic runs.</p> <p>The Diagnostic automatically runs on each applicable Source Node in the specified Node Group if the incident has the Lifecycle State currently configured in this attribute of the Diagnostic (Flow Definition - set of automated commands).</p>
Last Update Time	<p>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.</p>

## Node Form: Incidents Tab

**Tip:** See "[Incident Form](#)" on page 311 for more details about the incident attributes that appear in the incident table view's column headings.

The "[Node Form](#)" on page 50 provides details about the selected node.

**For information about each tab:**

### Incidents Table









Description
<p>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.</p> <p>Double-click the row representing an incident. The "<a href="#">Incident Form</a>" on page 311 displays all details about the selected incident.</p>

## Node Form: Status Tab

The "Node Form" on page 50 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 interface health contribute to node status. For information about how the current status was determined, see the <a href="#">"Node Form: Conclusions Tab" on the next page</a>. Status reflects the most serious outstanding conclusion. See <a href="#">"Watch Status Colors" on page 285</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</li></ul>

### Overall Status, continued

Attribute	Description
	<p>Conclusion Status is Normal.</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 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>Double-click the row representing a Status History. The Status History form displays all details about the selected Status.</p>

## Node Form: Conclusions Tab

The "Node Form" on page 50 provides details about the selected node.

All relevant Conclusions are shown in the table on this tab. The most severe Status in the current group of conclusions becomes the overall Node status. Some Node conclusions for routers can propagate to relevant Router Redundancy Groups:

**For information about each tab:**

### Outstanding Status Conclusion Values

Attribute	Description
Outstanding Status Conclusions	<p>The dynamically generated list of summary statuses of the node that contributed to the current overall Status of the selected node. 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>The Status value is correlated based on the most critical Conclusions.</p> <p>Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion.</p> <p>The following table describes the possible Conclusions that might appear for a node object.</p> <p><b>Note:</b> A <b>Y</b> in the <b>Incident?</b> column indicates that the Conclusion results in an</p>

**Outstanding Status Conclusion Values, continued**

Attribute	Description																				
	<p>incident.</p> <p><b>Critical Status Conclusions</b></p> <table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>CustomPollingOnNodeCritical</td> <td>At least one Custom Polled Instance associated with the physical node has a Status of Critical.</td> <td>Critical</td> <td>N</td> </tr> <tr> <td>NodeDown</td> <td> <p>The NNMi Causal Engine has determined the node is down based on the following analysis:</p> <ul style="list-style-type: none"> <li>• 100% of the addresses assigned to this node are unreachable</li> <li>• The SNMP agent installed on this machine is not responding</li> <li>• NNMi is communicating with at least two of the neighboring devices.</li> </ul> </td> <td>Critical</td> <td>Y</td> </tr> <tr> <td>NodeOrConnectionDown</td> <td>A node is not responding to an ICMP or SNMP query. It also indicates that NNMi is communicating with only one neighbor. Therefore, NNMi cannot determine whether the node or the connection is down.</td> <td>Critical</td> <td>Y</td> </tr> <tr> <td>NonSNMPNodeUnresponsive</td> <td>A non-SNMP node is unresponsive. Reasons for this include: 1) The node is down, or 2) An undiscovered device in the path between the node and the NNMi management server is down.</td> <td>Critical</td> <td>Y</td> </tr> </tbody> </table>	Conclusion	Description	Status	Incident?	CustomPollingOnNodeCritical	At least one Custom Polled Instance associated with the physical node has a Status of Critical.	Critical	N	NodeDown	<p>The NNMi Causal Engine has determined the node is down based on the following analysis:</p> <ul style="list-style-type: none"> <li>• 100% of the addresses assigned to this node are unreachable</li> <li>• The SNMP agent installed on this machine is not responding</li> <li>• NNMi is communicating with at least two of the neighboring devices.</li> </ul>	Critical	Y	NodeOrConnectionDown	A node is not responding to an ICMP or SNMP query. It also indicates that NNMi is communicating with only one neighbor. Therefore, NNMi cannot determine whether the node or the connection is down.	Critical	Y	NonSNMPNodeUnresponsive	A non-SNMP node is unresponsive. Reasons for this include: 1) The node is down, or 2) An undiscovered device in the path between the node and the NNMi management server is down.	Critical	Y
Conclusion	Description	Status	Incident?																		
CustomPollingOnNodeCritical	At least one Custom Polled Instance associated with the physical node has a Status of Critical.	Critical	N																		
NodeDown	<p>The NNMi Causal Engine has determined the node is down based on the following analysis:</p> <ul style="list-style-type: none"> <li>• 100% of the addresses assigned to this node are unreachable</li> <li>• The SNMP agent installed on this machine is not responding</li> <li>• NNMi is communicating with at least two of the neighboring devices.</li> </ul>	Critical	Y																		
NodeOrConnectionDown	A node is not responding to an ICMP or SNMP query. It also indicates that NNMi is communicating with only one neighbor. Therefore, NNMi cannot determine whether the node or the connection is down.	Critical	Y																		
NonSNMPNodeUnresponsive	A non-SNMP node is unresponsive. Reasons for this include: 1) The node is down, or 2) An undiscovered device in the path between the node and the NNMi management server is down.	Critical	Y																		

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	<b>Major Status Conclusions</b>			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
	CustomPollingOnNodeMajor	At least one Custom Polled Instance associated with the physical node has a Status of Major.	Major	N
	NodeWithBadBackplane	At least one of the monitored attributes for the backplane on the node is outside of the threshold range set on the device.	Major	N
	NodeWithBadFan	At least one of the monitored attributes for a fan on the node is outside of the threshold range set on the device.	Major	N
	NodeWithBadMemory	At least one memory pool on the node is outside the threshold range configured for the device. This incident indicates the memory pool is exhausted or cannot meet the demand for use.	Major	N
	NodeWithBadPowerSupply	At least one of the power supply's monitored attributes on the node is outside of the threshold range set on the device.	Major	N
	<b>Minor Status Conclusions</b>			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
	AllUnresponsiveAddressesInNode	None of the addresses associated with the selected node respond to ICMP ping.	Minor	N

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
	CardsDownInNode	At least one card in the node has an Operational State of Down.	Minor	N
	CardsUndeterminedStateInNode	At least one card in the node has an Operational State of Other. This state indicates the card is not functioning. For example, the card has a bad loop problem.	Minor	N
	CustomPollingOnNodeMinor	At least one Custom Polled Instance associated with the physical node has a Status of Minor.	Minor	N
	InterfacesDownInNode	At least one interface contained in the node	Minor	N

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		has an Operational State of Down.		
	SNMPAgentPingUnresponsiveInNode	The management address on the node is not responding to ICMP.	Minor	N
	SomeInterfacesOutsideThresholdBoundariesInNode	At least one interface on the node has a threshold outside the range specified for the device.	Minor	N
	SomeUnresponsiveAddressesInNode	At least one, but not all addresses, in the node are not responding to ICMP.	Minor	N
	UnresponsiveAgentInNode	The SNMP Agent associated with this node is not responding to SNMP requests.	Minor	N
<b>Warning Status Conclusions</b>				



**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
	CrgMalfunctionInNode	A Card Redundancy Group in the node has a Status other than Normal.	Warning	N
	CustomPollingOnNodeWarning	At least one Custom Polled Instance associated with the physical node has a Status of Warning.	Warning	N
	<b>Unknown Status Conclusions</b>			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
	NodeUnmanageable	<p>The node cannot be reached because NNMi has determined that the node on which it depends to route its traffic is down. This condition is known as “in the shadow”.</p> <p>Note: The status of any node “in the shadow” of a node that is down is always Unknown and the conclusion on each of the nodes in the shadow is NodeUnmanageable.</p>	Unknown	N
	<b>Normal Status Conclusions</b>			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
	AllInterfacesWithinThresholdBoundariesInNode	All of the interfaces within the selected node are within the allowable threshold range configured by the administrator	Normal	N

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		r.		
	AllResponsiveAddressesInNode	All of the addresses associated with the selected node respond to ICMP ping.	Normal	N
	CardsUpInNode	All cards in the node have an Operational State of Up.	Normal	N
	CrgNormalInNode	All Card Redundancy Groups in the node are functioning properly.	Normal	N
	CustomPollingOnNodeNormal	All Custom Polled Instances associated with the physical node have a Status of Normal.	Normal	N
	InterfacesUpInNode	All interfaces in the node have an Operational State of Up.	Normal	N
	NodeUp	The node and its components are	Normal	N

### Outstanding Status Conclusion Values, continued

Attribute	Description			
	Conclusion	Description	Status	Incident?
		functioning properly.		
	ResponsiveAgentInNode	The node's SNMP Agent is responding.	Normal	N
	<p>Multiple Node conclusions can appear for the same node object. For example, if a node is functioning properly and it has monitored addresses, interfaces, at least one card, and a card redundancy group, you would see these conclusions together:</p> <ul style="list-style-type: none"> <li>• SNMPAgentResponding</li> <li>• AllResponsiveAddressesInNode</li> <li>• InterfacesUpInNode</li> <li>• CardsUpInNode</li> <li>• CrgNormalInNode</li> </ul>			

## Node Form: Registration Tab

The "Node Form" on page 50 provides details about the selected node.

For information about each tab:

### Registration Attributes

Attribute	Description
Created	<p>Date and time the Node object instance was created. NNM uses the locale of the client and the date and time from the NNMi management server.</p> <p><b>Note:</b> This value does not change when a node is rediscovered. This is because the Node object is modified, but not created.</p>
Last Modified	<p>Date and time the Node object instance was last modified. NNM uses the locale of the client and the date and time from the NNMi management server.</p> <p>Note the following:</p> <ul style="list-style-type: none"> <li>• When a node is rediscovered, the Last Modified time is the same as the Discovery Completed time. This is because the node's Discovery State changes from Started to Completed.</li> <li>• When a Node is initially discovered, the Last Modified time is slightly later than the Created time. This is because node discovery does not complete until after the Node is created.</li> </ul>

### Object Identifiers Attributes

Attribute	Description
ID	The Unique Object Identifier, which is unique within the NNMi database.
UUID	The Universally Unique Object Identifier, which is unique across all databases.




## Device Profile Form

According to industry standards (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.

**Tip:** Each "Node Form" on page 50 has a link to the appropriate Device Profile form.

### Basic Attributes

Attribute	Description
Device Model	Device model name or number designator, determined by the vendor.
SNMP Object ID	MIB-II <i>sysObjectID</i> number issued for this device type. These numbers are unique across all vendors.
Description	The description, based on information from the MIB-II <i>sysDescr</i> string provided by the vendor.  Maximum length is 255 characters: alpha-numeric, spaces, and special characters (~!@#\$%^&*()_+)
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 "Device Family Form" on page 88 for more details.
Device Vendor	Name of the vendor that manufactures the device.  Click the  Lookup icon to access the "Device Vendor Form" on page 89 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 "Device Category Form" on page 89 for more details.

**Basic Attributes , continued**

Attribute	Description
OUI	Organizationally unique identifier. The first three octets of the MAC address for the device that identify the device's vendor.
Author	<p>Indicates who created or last modified the device profile.</p> <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <p><b>Caution:</b> If the Author attribute value is <b>HP Network Node Manager</b>, any changes are at risk of being overwritten in the future.</p> </div> <ul style="list-style-type: none"> <li>• Click  <b>Lookup</b> and select  <b>Show Analysis</b> to display details about the currently selected Author.</li> <li>• Click  <b>Quick Find</b> to access the list of existing Author values.</li> <li>• Click  <b>New</b> to create an Author value.</li> </ul>

**Advanced Settings Tab**

Attribute	Description
<b>Use of SNMP SysName for Node Name Resolution</b>	
Never Use sysName	<p>If <input checked="" type="checkbox"/> enabled, Spiral Discovery does not use a MIB-II <code>sysName</code> value for the Name attribute for discovered Nodes of this type. If <code>sysName</code> 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 <b>sysName</b> 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 <code>sysName</code> text string, from MIB-II <code>sysName</code>.</p> <p>If the SNMP agent responds to a <code>sysName</code> request with a value that matches or starts with the entry in this field (case-sensitive), Spiral Discovery ignores the <code>sysName</code> and considers <code>sysName</code> 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 <code>sysName</code>, 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 <code>sysName</code>). Usually, the device administrator changes the default <code>sysName</code> 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) Capability settings provided by Spiral Discovery (displayed on the "Node Form: Capabilities Tab" on page 63).</p> <p>Note the following:</p>

**Advanced Settings Tab , continued**

Attribute	Description												
	<ul style="list-style-type: none"> <li>The Force Device attribute does not affect default membership for the Node Groups provided by NNMi. For example, the <b>Force to router</b> settings does not add the Node to the Routers Node Group. NNMi uses the Device Category to determine Node Group membership for the Node Groups it provides.</li> <li>The Force Device setting does not affect the background shapes displayed on an NNMi map. NNMi uses the Device Category specified in the Device Profile to determine the map background shapes displayed.</li> </ul> <p>The following table describes the possible Force Device settings and subsequent behavior:</p> <p><b>Force Device Settings and Behavior</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #003366; color: white;">Setting</th> <th style="background-color: #003366; color: white;">Behavior</th> </tr> </thead> <tbody> <tr> <td>Do not force</td> <td>Ignores the Force Device setting.</td> </tr> <tr> <td>Force to router</td> <td> <ul style="list-style-type: none"> <li>Adds the IP Forwarding (Layer 3) Capability to the Node</li> <li>Displays the device in Layer 3 Neighbor View maps</li> <li>Checks the Router Redundancy Protocol configuration for information about the Node</li> </ul> </td> </tr> <tr> <td>Force to switch</td> <td>Adds the LAN Switching (Layer 2) Capability to the Node</td> </tr> <tr> <td>Force to end node</td> <td> <ul style="list-style-type: none"> <li>Removes either of the following Capabilities if they are configured on the Node:                             <ul style="list-style-type: none"> <li>IP Forwarding (Layer 3)</li> <li>LAN Switching (Layer 2)</li> </ul> </li> <li>Ignores this Node during Auto-Discovery unless you select "Discover Any SNMP Device" or include the Node's System Object ID in the Auto-Discovery Rule.</li> </ul> </td> </tr> <tr> <td>Force to switch and router</td> <td> <ul style="list-style-type: none"> <li>Adds the IP Forwarding (Layer 3) Capability to the Node</li> <li>Adds the LAN Switching (Layer 2) Capability to the Node</li> <li>Displays the Node in Layer 3 Neighbor View maps</li> <li>Checks the Router Redundancy Protocol configuration for information about the Node</li> </ul> </td> </tr> </tbody> </table> <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 <code>sysServices</code> setting in MIB-II that is used to determine the IP Forwarding (Layer 3) and LAN Switching (Layer 2) capability during discovery is not</li> </ul>	Setting	Behavior	Do not force	Ignores the Force Device setting.	Force to router	<ul style="list-style-type: none"> <li>Adds the IP Forwarding (Layer 3) Capability to the Node</li> <li>Displays the device in Layer 3 Neighbor View maps</li> <li>Checks the Router Redundancy Protocol configuration for information about the Node</li> </ul>	Force to switch	Adds the LAN Switching (Layer 2) Capability to the Node	Force to end node	<ul style="list-style-type: none"> <li>Removes either of the following Capabilities if they are configured on the Node:                             <ul style="list-style-type: none"> <li>IP Forwarding (Layer 3)</li> <li>LAN Switching (Layer 2)</li> </ul> </li> <li>Ignores this Node during Auto-Discovery unless you select "Discover Any SNMP Device" or include the Node's System Object ID in the Auto-Discovery Rule.</li> </ul>	Force to switch and router	<ul style="list-style-type: none"> <li>Adds the IP Forwarding (Layer 3) Capability to the Node</li> <li>Adds the LAN Switching (Layer 2) Capability to the Node</li> <li>Displays the Node in Layer 3 Neighbor View maps</li> <li>Checks the Router Redundancy Protocol configuration for information about the Node</li> </ul>
Setting	Behavior												
Do not force	Ignores the Force Device setting.												
Force to router	<ul style="list-style-type: none"> <li>Adds the IP Forwarding (Layer 3) Capability to the Node</li> <li>Displays the device in Layer 3 Neighbor View maps</li> <li>Checks the Router Redundancy Protocol configuration for information about the Node</li> </ul>												
Force to switch	Adds the LAN Switching (Layer 2) Capability to the Node												
Force to end node	<ul style="list-style-type: none"> <li>Removes either of the following Capabilities if they are configured on the Node:                             <ul style="list-style-type: none"> <li>IP Forwarding (Layer 3)</li> <li>LAN Switching (Layer 2)</li> </ul> </li> <li>Ignores this Node during Auto-Discovery unless you select "Discover Any SNMP Device" or include the Node's System Object ID in the Auto-Discovery Rule.</li> </ul>												
Force to switch and router	<ul style="list-style-type: none"> <li>Adds the IP Forwarding (Layer 3) Capability to the Node</li> <li>Adds the LAN Switching (Layer 2) Capability to the Node</li> <li>Displays the Node in Layer 3 Neighbor View maps</li> <li>Checks the Router Redundancy Protocol configuration for information about the Node</li> </ul>												

**Advanced Settings Tab , continued**

Attribute	Description
	<p>accurate due to a firmware defect on the device.</p> <ul style="list-style-type: none"> <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> <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 Spiral Discovery to ignore this device (unless the device is within the Default Tenant and an Auto-Discovery Rule is configured to "Discover Any SNMP Device" or configured to include the matching System Object ID).</p>
Interface Reindexing Type	<p>Your NNMi administrator chooses which interface MIB variable the NNMi State Poller queries to detect interface changes. NNMi can use the following MIB-II attribute values: <code>ifIndex</code>, <code>ifName</code>, <code>ifDescr</code>, <code>ifAlias</code>, or a combination of these (<code>ifName</code> or <code>ifDescr</code>, <code>ifName</code> or <code>ifDescr</code> or <code>ifAlias</code>). See the General Interface Attributes (SNMP Values) in "<a href="#">Interface Form: General Tab</a>" on page 95 for information about these four MIB-II attributes that are available to use for this setting.</p> <p>If you are an Administrator, see <a href="#">Detect Interface Changes</a> for more information.</p>
Prefer LLDP	<p>A network device's interfaces can be configured with proprietary Layer 2 <i>discovery protocols</i>, instead of or in addition to the industry standard LLDP (see the list of Topology Source protocols in <a href="#">Layer 2 Connection Form</a>).</p> <p>By default, NNMi checks the interface for standard LLDP and vendor-specific IEEE 802 Layer 2 protocol. NNMi uses data from both protocols to calculate the Layer 2 Connection, but by default prefers the data provided through LLDP.</p> <p><b>Note:</b> Forwarding Database (FDB) information can cause NNMi to establish wrong Layer 2 Connections in the following cases:</p> <ul style="list-style-type: none"> <li>When the FDB is configured as cache and contains obsolete data.</li> <li>In network environments with hardware from a variety of vendors, when each vendor generates different and sometimes conflicting FDB data.</li> </ul> <p><i>Optional:</i> NNMi administrators can configure Spiral Discovery to ignore the FDB data from one Node Group when calculating Layer 2 Connections (the FDB data is still included in other calculations).</p> <p>(<i>NNMi Advanced - Global Network Management feature</i>) NNMi must read the Forwarding Database (FDB) tables from Ethernet switches within the network before accurate communication paths between these network devices can be calculated. Because the FDB data is involved, NNMi can produce different results on a Regional Manager as opposed to the Global Manager.</p> <p>If NNMi discovers more than one IEEE 802 Layer 2 protocol being used by a</p>

### Advanced Settings Tab , continued

Attribute	Description
	<p>particular device's interface, the Device Profile's setting controls NNMi's protocol preference:</p> <p><input checked="" type="checkbox"/> <b>Prefer LLDP = Enabled:</b> NNMi gives priority to the LLDP data.</p> <p><input type="checkbox"/> <b>Prefer LLDP = Disabled:</b> NNMi gives priority to the vendor-specific IEEE 802 Layer 2 protocol data.</p> <p><b>Tip:</b> If NNMi detects incorrect neighbors, make sure that the interfaces at both ends of the Layer 2 Connection are using the same configuration for Layer 2 discovery protocol. For more information, see <a href="#">Troubleshooting Layer 2 Connections</a>.</p>

## 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 84.

### Device Family Definition

Attribute	Description
Label	<p>Device family name. For example, Cisco Catalyst 6500 Series Switches or HP AdvanceStack Routers.</p> <p>Maximum length is 255 characters. Alpha-numeric, spaces, and underline characters are permitted.</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.device_ profile.family.&lt;family_label&gt;</pre> <p>Maximum length is 80 characters. Alpha-numeric characters and periods are permitted. Spaces are not permitted.</p>
Management URL	<p><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.</p>
Icon	<p>Displays the icon that is associated with the Device Family.</p> <p>If you are an NNMi administrator, you can customize the icon. See <a href="#">Customize Device Profile Icons</a> for more information.</p>



## 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 84.

### Device Vendor Definition

Attribute	Description
Label	Vendor name.  Maximum length is 255 characters. Alpha-numeric, spaces, and underline characters are permitted.
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.device_profile.vendor.&lt;vendor_label&gt;</code>  Maximum length is 80 characters. Alpha-numeric characters and periods are permitted. Spaces are not permitted.
Icon	Displays the icon that is associated with the Device Vendor.  If you are an NNMi administrator, you can customize the icon. See <a href="#">Customize Device Profile Icons</a> for more information.

## 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 84.

## Device Category Definition

Attribute	Description
Label	Category name.  Maximum length 255 is characters. Alpha-numeric, spaces, and underline characters are permitted.
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.device_profile.category.&lt;category_label&gt;</code>  Maximum length is 80 characters. Alpha-numeric characters and periods are permitted. Spaces are not permitted.
Icon	Displays the icon that is associated with the Device Category.  If you are an NNMi administrator, you can customize the icon. See <a href="#">Customize Device Profile Icons</a> for more information.

## 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 permits, 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 columns for an interface in a table view, note the following:

- The interface might be in a non-SNMP node.  
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**.

**Note:** For **Pseudo Interface**, NNMi attempts to obtain additional information using a variety of *discovery protocols* (see the list of Topology Source protocols in [Layer 2 Connection Form](#)).

- 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.
- The interface might be a Nortel private interface.

For Nortel SNMP interfaces, note the following:

- The interface index (`ifIndex`) value is set according the Nortel private MIB.
- NNMi tries to collect the MAC address and interface name using Nortel's private MIBs.
- (NNMi Advanced) The interface might be an IPv-6 interface.









A small number of IPv6 devices do not support the standard RFC 2863 IF-MIB for IPv6 interfaces. In this case, NNMi uses the *RFC 2465 IPv6-MIB*. When this happens, note the following:

- Interface index (`ifIndex`) and description (`ifDescr`) are set according to the RFC 2465 IPv6 MIB.
- Interface type (`ifType`) is set to `Other` (no specific type is available).
- Interface Name (`ifName`), Alias (`ifAlias`), and Speed (`ifSpeed`) are blank (not available).
- NNMi monitors the Status of this interface, but Performance metrics are not available.




When an IP Address has the Interface Name (`ifName`) attribute set to blank, NNMi constructs an alternate string for the IP Address's **In Interface** attribute (`Other [<ifIndex_value>]`).

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 "Interface Form: Status Tab" on page 115 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>








**Basic Attributes, continued**

Attribute	Description
	<p>Interface status is derived from SNMP polling results for <code>ifAdminStatus</code> and <code>ifOperStatus</code>, as well as from any conclusions. Status reflects the most serious outstanding conclusion. See the "<a href="#">Interface Form: Conclusions Tab</a>" on page 116 for information about how the current status was determined. See "<a href="#">Watch Status Colors</a>" on page 285 for more information about possible status values.</p> <p><b>Note:</b> The icons are displayed only in table views.</p>
<p>Management Mode</p>	<p>The calculated Management Mode for the interface. This value should reflect the management mode assigned to the node in 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> <p><i>(NNMi Advanced - Global Network Management feature)</i> Any change to this Management Mode setting is sent from a Regional Manager to the Global Manager during the next Spiral Discovery cycle on the Regional Manager.</p> <p><b>Note:</b> If the NNMi Security configuration permits, you can change this setting using <b>Actions</b> → <b>Management Mode</b>.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Tip:</b> You can right-click any object in a table or map view to access the <b>Actions</b> menu.</p> </div>
<p>Direct Management Mode</p>	<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> <ul style="list-style-type: none"> <li> <b>Inherited</b> – Used to indicate that the interface should inherit the Management Mode from the node in which it resides.</li> <li> <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.</li> <li> <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.</li> </ul> <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 using <b>Actions</b> → <b>Management Mode</b>, 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>
<p>Hosted On Node</p>	<p>node in 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</p>














### Basic Attributes, continued

Attribute	Description
	<p>administrator configured the discovery process).</p> <p>Click the  Lookup icon and select  Show Analysis 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> <li>2. In the Layer 2 Connection form, locate the <b>Interfaces</b> tab.</li> <li>3. Double-click the row representing 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

Attribute	Description
Administrative State	<p>Either the current MIB-II <i>ifAdminStatus</i> 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 "<a href="#">Interface Form: Status Tab</a>" on page 115 for more information.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> <li> <b>Up</b> – The SNMP agent responded with an <i>ifAdminStatus</i> value of Up. The interface is ready to pass packets of data.</li> <li> <b>Down</b> – The SNMP agent responded with an <i>ifAdminStatus</i> value of Down.</li> <li> <b>Testing</b> – The SNMP agent responded that the interface is in test mode.</li> <li> <b>Other</b> – The SNMP agent responded with a value for <i>ifAdminStatus</i> that is not recognized.</li> </ul> <p>The following values indicate NNMi could not gather the required data:</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 this agent.</li> <li> <b>No Polling Policy</b> - Indicates the object is being polled, but no polling policy exists in Monitoring Configuration settings for this monitored attribute.</li> <li> <b>Not Polled</b> - Indicates that this attribute is intentionally not polled, based on</li> </ul>

**Interface State Attributes, continued**

Attribute	Description
	<p>current Monitoring Configuration settings, current Communication Configuration settings, or because the parent Node is set to Not Managed or Out of Service. This object attribute might or might not have an associated polling policy.</p> <p> <b>Unavailable</b> - Unable to determine the State. For example, the SNMP agent returned a value outside the range of possible values or returned a null value.</p> <p> <b>Unset</b> – Currently not used by NNMi.</p>
Operational State	<p>Either the current MIB-II <i>ifOperStatus</i> value or a value calculated by the State Poller Service. The current Operational State contributes towards the status calculation for this interface. See the "<a href="#">Interface Form: Status Tab</a>" on page 115 for more information.</p> <p>Possible values are:</p> <p> <b>Up</b> – The SNMP agent responded that the interface is operationally up, ready to receive and send network traffic.</p> <p> <b>Down</b> – The SNMP agent responded that the interface is operationally down.</p> <p> <b>Dormant</b> – Indicates the SNMP agent responded that the interface is in a "pending" state, waiting for some external event.</p> <p> <b>Lower Layer Down</b> – Indicates the interface is down due to the state of lower-level interfaces.</p> <p> <b>Minor Fault</b> – The interface is still functional, but the SNMP agent reported a minor concern. Check the device, itself, for more details.</p> <p> <b>Not Present</b> – Indicates that the interface is missing some hardware component.</p> <p> <b>Other</b> – The SNMP agent responded with a value for <i>ifOperStatus</i> that is not recognized.</p> <p> <b>Testing</b> – The SNMP agent responded that the interface is in test mode.</p> <p> <b>Unknown</b> – The SNMP agent responded with an <i>ifOperStatus</i> value of Unknown.</p> <p>The following values indicate NNMi could not gather the required data:</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 the object is being polled, but no polling policy exists in Monitoring Configuration settings for this monitored attribute.</p>

### Interface State Attributes, continued

Attribute	Description
	<p> <b>Not Polled</b> - Indicates that this 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. This object attribute might or might not have an associated polling policy.</p> <p> <b>Unavailable</b> - Unable to determine the State. For example, the SNMP agent returned a value outside the range of possible values or returned a null value.</p> <p> <b>Unset</b> – Currently not used by NNMi.</p>
State Last Modified	<p><i>(NNMi Advanced - Global Network Management feature)</i> The text you enter here is not sent from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager can add notes that are stored in the NNMi database on the Global Manager.</p> <p>The date and time when the Administrative State, Operational State, or both were last modified.</p>
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, spaces, and special characters (~ ! @ # \$ % ^ &amp; * ( ) _ + -) are permitted.</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 90 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.
ifDescr	Optional Interface MIB variable for ifDescr for the interface. This attribute is set by the device administrator.

**General SNMP Values, continued**

Attribute	Description
ifIndex	<p>Interface MIB variable for the row number in the interface table (ifTable) for this interface. The row number can change. If you are an Administrator, see <a href="#">Accurately Detect Interface Changes</a> for more information.</p> <p><b>Note:</b> Interfaces on non-SNMP nodes have an ifIndex value of 0 (zero).</p>
ifSpeed	<p>Interface MIB variable for the interface's bandwidth in bits per second. Depending on the device vendor, this value might indicate current speed or potential speed.</p>
ifType	<p>Interface MIB variable for the physical link protocol type of the interface. Possible values include: <code>Ethernet</code> and <code>frameRelay</code>.</p> <p><b>Note:</b> Interfaces on non-SNMP nodes have an ifType value of <code>other</code>.</p>
Input Speed	<p><i>(NNM iSPI Performance for Metrics)</i> If the HP Network Node Manager iSPI Performance for Metrics Software is installed and configured within your environment, you can type an integer value to override the input speed value returned by the device's SNMP agent. Indicate the speed this interface is capable of receiving data in bits per second.</p> <p>For example, you might want to override the Input Speed value for the following reason:</p> <p>Sometimes the value returned by the device's SNMP agent is not accurate or causes problems when NNM iSPI Performance for Metrics 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).</p> <p><b>Note:</b> <i>(NNMi Advanced - Global Network Management)</i> If you change this value for an Interface monitored by a Regional Manager, NNMi forwards the updated information to the Global Manager at the next Discovery Interval.</p> <p>If you are an NNMi administrator, you can set input speeds for multiple interfaces using the <code>nnmsetiospeed.ovpl</code> command. Also see "Maintaining NNMi" in the HP Network Node Manager i Software Deployment Reference for more information.</p>
Output Speed	<p><i>(NNM iSPI Performance for Metrics)</i> If the HP Network Node Manager iSPI Performance for Metrics Software is installed and configured within your environment, you can type an integer value to override the output speed value returned by the device's SNMP agent. Indicate the speed this interface is capable of transmitting data in bits per second.</p> <p>For example, you might want to override the Output Speed value for the following reason:</p> <p>Sometimes the value returned by the device's SNMP agent is not accurate or causes</p>



### General SNMP Values, continued

Attribute	Description
	<p>problems when NNM iSPI Performance for Metrics 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).</p> <p><b>Note:</b> (<i>NNMi Advanced - Global Network Management</i>) If you change this value for an Interface monitored by a Regional Manager, NNMi forwards the updated information to the Global Manager at the next Discovery Interval.</p> <p>If you are an NNMi administrator, you can set output speeds for multiple interfaces using the <code>nnmsetiospeed.ovpl</code> command. Also see "Maintaining NNMi" in the <i>HP Network Node Manager i Software Deployment Reference</i> for more information.</p>

## Interface Form: IP Addresses Tab

The "Interface Form" on page 90 provides details about the selected network interface.

For information about each tab:

### IP Addresses Table

Attribute	Description
IP Address	<p>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.</p> <p>Double-click the row representing an IP address. The "IP Address Form" on page 132 displays all details about the selected IP address.</p>

## Interface Form: Ports Tab

The "Interface Form" on page 90 provides details about the selected network interface.

For information about each tab:

### Ports Table

Attribute	Description
Ports	<p>Table view of all of the ports associated with the selected interface. Use this table to access information about each port associated with the selected interface.</p> <p>Double-click the row representing a port. The "Port Form" on page 171 displays all details about the selected port.</p>

## Interface Form: VLAN Ports Tab

The "Interface Form" on page 90 provides details about the selected network interface.

For information about each tab:

(*NNMi Advanced - Global Network Management feature*) There might be slight differences between the VLAN information shown on Regional Managers and Global Managers, because the VLAN calculations use [Layer 2 Connections](#) data.

### VLAN Ports Table

Attribute	Description
VLAN Ports	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.  Double-click the row representing a VLAN port. The "VLAN Port Form" on page 62 displays all details about the selected VLAN port.

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

The "Interface Form" on page 90 provides details about the selected network interface.

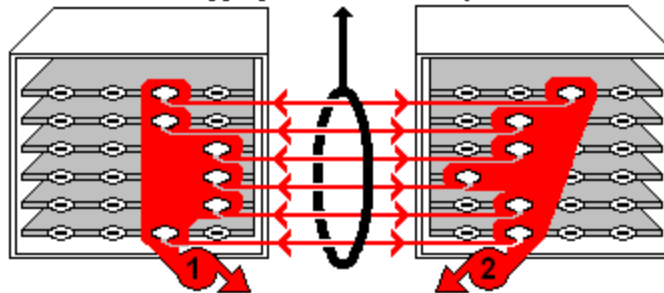
For more information about each tab:

The Interface Form: Link Aggregation Tab appears if the selected interface uses a [Link Aggregation](#)<sup>1</sup> protocol.

### Example Link Aggregation

Thick Line on Layer 2 Neighbor View Map =  
one Aggregator Layer 2 Connection:

- Logical unit (not physical)
- Functions as if it were one
- 6 Aggregation Member Layer 2 Connections



two Aggregator Interfaces:

- Logical units (not physical)
- Each functions as if it were one
- Each has 6 Aggregation Member Interfaces



<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

The selected object's *role* in the Link Aggregation determines the contents of the tab:

- **Aggregation Member**, click here for details.

Attribute	Description																
Link Aggregation Protocol	<p>The <b>Link Aggregation</b><sup>1</sup> Protocol currently in use. These protocols allow network administrators to configure a <i>set of interfaces</i> on a switch as one <i>Aggregator Interface</i>, creating an Aggregator Layer 2 Connection to another device using multiple interfaces in parallel to increase bandwidth, increase the speed at which data travels, and increase redundancy:</p> <table border="1" data-bbox="483 491 1377 1157"> <thead> <tr> <th data-bbox="483 491 873 548">Text</th> <th data-bbox="873 491 1377 548">Represents This Protocol</th> </tr> </thead> <tbody> <tr> <td data-bbox="483 548 873 642">Cisco Port Aggregation Protocol</td> <td data-bbox="873 548 1377 642">Cisco Systems Port Aggregation Protocol (pagp)</td> </tr> <tr> <td data-bbox="483 642 873 699">Nortel Multi-Link Trunking</td> <td data-bbox="873 642 1377 699">Nortel Multi-Link Trunk technology (mlt)</td> </tr> <tr> <td data-bbox="483 699 873 793">Split MLT</td> <td data-bbox="873 699 1377 793">Split Multi-Link Trunk: configuration technology (splitMlt)</td> </tr> <tr> <td data-bbox="483 793 873 888">Inter-Switch Trunk MLT</td> <td data-bbox="873 793 1377 888">Split Multi-Link Trunk: inter-switch trunk (istMlt)</td> </tr> <tr> <td data-bbox="483 888 873 982">802.3ad Link Aggregation Control Protocol</td> <td data-bbox="873 888 1377 982">IEEE 802.3ad Link Aggregation Control protocol (LACP)</td> </tr> <tr> <td data-bbox="483 982 873 1077">Static/Manual Configured Link Aggregation</td> <td data-bbox="873 982 1377 1077">Static/Manual Configured Link Aggregation</td> </tr> <tr> <td data-bbox="483 1077 873 1157">Unknown Protocol Link Aggregation</td> <td data-bbox="873 1077 1377 1157">unknown</td> </tr> </tbody> </table> <p><b>Note:</b> It is possible for a Layer 2 Connection to connect sets of Aggregator/Member Interfaces that are configured using different Link Aggregation protocols. In that case, this attribute value contains multiple protocols separated with a slash (/).</p>	Text	Represents This Protocol	Cisco Port Aggregation Protocol	Cisco Systems Port Aggregation Protocol (pagp)	Nortel Multi-Link Trunking	Nortel Multi-Link Trunk technology (mlt)	Split MLT	Split Multi-Link Trunk: configuration technology (splitMlt)	Inter-Switch Trunk MLT	Split Multi-Link Trunk: inter-switch trunk (istMlt)	802.3ad Link Aggregation Control Protocol	IEEE 802.3ad Link Aggregation Control protocol (LACP)	Static/Manual Configured Link Aggregation	Static/Manual Configured Link Aggregation	Unknown Protocol Link Aggregation	unknown
Text	Represents This Protocol																
Cisco Port Aggregation Protocol	Cisco Systems Port Aggregation Protocol (pagp)																
Nortel Multi-Link Trunking	Nortel Multi-Link Trunk technology (mlt)																
Split MLT	Split Multi-Link Trunk: configuration technology (splitMlt)																
Inter-Switch Trunk MLT	Split Multi-Link Trunk: inter-switch trunk (istMlt)																
802.3ad Link Aggregation Control Protocol	IEEE 802.3ad Link Aggregation Control protocol (LACP)																
Static/Manual Configured Link Aggregation	Static/Manual Configured Link Aggregation																
Unknown Protocol Link Aggregation	unknown																
Aggregator	<p>Name of the Aggregator that <i>contains</i> the selected participating Aggregation Member:</p> <ul style="list-style-type: none"> <li>■ Aggregator Interface - represents multiple member interfaces</li> <li>■ Aggregator Layer 2 Connection - thick line on the Layer 2 Neighbor View map represents multiple member Layer 2 Connections</li> </ul>																

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

Attribute	Description
	<p>See <a href="#">Layer 2 Neighbor View Map Objects</a> for more information.</p> <p>Click the  Lookup icon, and choose  Open to open the form for the Aggregator.</p>

- **Aggregator** (representing multiple members), click here for details.

Attribute	Description																
Link Aggregation Protocol	<p>The <b>Link Aggregation</b><sup>1</sup> Protocol currently in use. These protocols allow network administrators to configure a <i>set of interfaces</i> on a switch as one <i>Aggregator Interface</i>, creating an Aggregator Layer 2 Connection to another device using multiple interfaces in parallel to increase bandwidth, increase the speed at which data travels, and increase redundancy:</p> <table border="1" data-bbox="483 724 1377 1388"> <thead> <tr> <th>Text</th> <th>Represents This Protocol</th> </tr> </thead> <tbody> <tr> <td>Cisco Port Aggregation Protocol</td> <td>Cisco Systems Port Aggregation Protocol (pagp)</td> </tr> <tr> <td>Nortel Multi-Link Trunking</td> <td>Nortel Multi-Link Trunk technology (mlt)</td> </tr> <tr> <td>Split MLT</td> <td>Split Multi-Link Trunk: configuration technology (splitMlt)</td> </tr> <tr> <td>Inter-Switch Trunk MLT</td> <td>Split Multi-Link Trunk: inter-switch trunk (istMlt)</td> </tr> <tr> <td>802.3ad Link Aggregation Control Protocol</td> <td>IEEE 802.3ad Link Aggregation Control protocol (LACP)</td> </tr> <tr> <td>Static/Manual Configured Link Aggregation</td> <td>Static/Manual Configured Link Aggregation</td> </tr> <tr> <td>Unknown Protocol Link Aggregation</td> <td>unknown</td> </tr> </tbody> </table> <p><b>Note:</b> It is possible for a Layer 2 Connection to connect sets of Aggregator/Member Interfaces that are configured using different Link Aggregation protocols. In that case, this attribute value contains multiple protocols separated with a slash (/).</p>	Text	Represents This Protocol	Cisco Port Aggregation Protocol	Cisco Systems Port Aggregation Protocol (pagp)	Nortel Multi-Link Trunking	Nortel Multi-Link Trunk technology (mlt)	Split MLT	Split Multi-Link Trunk: configuration technology (splitMlt)	Inter-Switch Trunk MLT	Split Multi-Link Trunk: inter-switch trunk (istMlt)	802.3ad Link Aggregation Control Protocol	IEEE 802.3ad Link Aggregation Control protocol (LACP)	Static/Manual Configured Link Aggregation	Static/Manual Configured Link Aggregation	Unknown Protocol Link Aggregation	unknown
Text	Represents This Protocol																
Cisco Port Aggregation Protocol	Cisco Systems Port Aggregation Protocol (pagp)																
Nortel Multi-Link Trunking	Nortel Multi-Link Trunk technology (mlt)																
Split MLT	Split Multi-Link Trunk: configuration technology (splitMlt)																
Inter-Switch Trunk MLT	Split Multi-Link Trunk: inter-switch trunk (istMlt)																
802.3ad Link Aggregation Control Protocol	IEEE 802.3ad Link Aggregation Control protocol (LACP)																
Static/Manual Configured Link Aggregation	Static/Manual Configured Link Aggregation																
Unknown Protocol Link Aggregation	unknown																

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

Attribute	Description
Available Bandwidth	Sum of the interface Input Speed attribute values of the Member Interfaces that have a MIB-II ifOperStatus that 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 Aggregation Members.</p> <p>For more information, double-click the row representing an Aggregation Member:</p> <ul style="list-style-type: none"> <li>■ The "Interface Form" on page 90 displays all details about the selected Interface.</li> <li>■ The "Layer 2 Connection Form" on page 188 displays all details about the selected Layer 2 Connection.</li> </ul>

## Interface Form: Capabilities Tab

The "Interface Form" on page 90 provides details about the selected interface.

### For information about each tab:

The Interface Form: Capabilities Tab displays a table view of any capabilities added to the interface object by 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.

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.

(*NNMi Advanced - Global Network Management feature*) Any Capability values added by an NNM iSPI are available on the Global Manager only if that iSPI is also running on the Global Manager.

### Capabilities Table

Attribute	Description
Capability	Table of all of the capabilities associated with the selected Interface. Use this table

### Capabilities Table, continued

Attribute	Description
	<p>to access information about each Capability.</p> <p>Double-click the row representing a Capability. The "Interface Capability Form" on page 110 displays all details about the selected Capability.</p> <p>For more information, see "Interface Capabilities Provided by NNMi" below.</p>

## Interface Capabilities Provided by NNMi

The "Interface Form: Capabilities Tab" on the previous page displays a table of any capabilities added to a particular interface object. Capabilities enable NNMi and application programmers to provide more information about an interface than what is initially stored in the NNMi database.

External applications can also add capabilities.

**KEY:** `com.hp.<product>.capability.<content>.<vendor/org>.<MIB/feature>`

Any Capability provided by NNMi begins with the prefix `com.hp.nnm.capability`.

`<product>` = Either NNMi or the NNM iSPI providing this capability.

`<content>` = card, ipaddr (address), iface (interface), lag ([Link Aggregation](#)<sup>1</sup> interface), node, rrp (Router Redundancy), or metric (Node Sensor, Component Health, Component and Device Metrics).

`<vendor/org>` = Standards organization or vendor defining the MIB or feature associated with the capability.

`<MIB/feature>` = What this capability measures.

**Note:** The following tables show a few examples of the Capabilities provided by NNMi.

### Interface Capability Attribute Values

Unique Key	Capability	Description
<code>com.hp.nnm.capability.iface.private</code>	Private	Indicates the interface was discovered in either a non-SNMP node or a Nortel node. Private interfaces are

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

Interface Capability Attribute Values, continued

Unique Key	Capability	Description
		<p>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> </ul> <div style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p><b>Note:</b> For <b>Pseudo Interface</b>, NNMi attempts to obtain additional information using a variety of <i>discovery protocols</i> (see the list of Topology Source protocols in <a href="#">Layer 2 Connection Form</a>).</p> </div> <ul style="list-style-type: none"> <li>• If the interface hosts an IP address, the interface Alias (<code>ifAlias</code>) is set to the IP address.</li> </ul>



**Interface Capability Attribute Values, continued**

Unique Key	Capability	Description
		<p>Otherwise, the interface Alias (<code>ifAlias</code>) is set with information from neighboring SNMP devices.</p> <ul style="list-style-type: none"> <li>• NNMi obtains the MAC address if the IP address can be resolved using ARP cache.</li> </ul> <p>For Nortel SNMP interfaces, note the following:</p> <ul style="list-style-type: none"> <li>• The interface index (<code>ifIndex</code>) 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>
<code>com.hp.nnm.capability.iface.ietf.DS1</code>	DS1 Interface Metrics	Interface that supports the DS1 (T1) MIB for gathering performance data. This data is used by NNM iSPI Performance for Metrics.
<code>com.hp.nnm.capability.iface.ietf.DS3</code>	DS3 Interface Metrics	Interface that supports the DS3 (T3) MIB for gathering performance data. This data is used by NNM iSPI Performance for Metrics.
<code>com.hp.nnm.capability.iface.ietf.ETHERLIKE</code>	EtherLike Interface Metrics	Interface that supports the Etherlike MIB for gathering performance

Interface Capability Attribute Values, continued

Unique Key	Capability	Description
		data. NNMi uses this MIB to monitor LAN errors. This data is used by NNM iSPI Performance for Metrics.
com.hp.nnm.capability.iface.ietf.IEEE80211	IEEE 802.11 Interface Metrics	Interface that supports the IEEE 802.11 Interface Metrics MIB. NNMi can monitor for WLAN metrics. This data is used by NNM iSPI Performance for Metrics.
com.hp.nnm.capability.iface.ietf.NON-DEFAULT-CONTEXT-RFC1213	RFC 1213 Interface from Non-default Context	<p>Indicates the following:</p> <ul style="list-style-type: none"> <li>• NNMi discovered the interface from the RFC1213 MIB.</li> <li>• The interface has a context other than default.</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• NNMi collects context values using the vacmContextTable in the SNMP-VIEW-BASED-ACM-MIB defined in RFC2575.</li> <li>• NNMi does not monitor interfaces under a non-default context.</li> </ul>

### Interface Capability Attribute Values, continued

Unique Key	Capability	Description
com.hp.nnm.capability.iface.PE	PE Interface	Indicates that the interface is serving as a Provider Edge (PE <sup>1</sup> ). NNMi's Subnet Connection Rules use this information.
com.hp.nnm.capability.iface.ietf.SONET	SONET Interface Metrics	Interface that supports the SONET-MIB interval monitoring metrics. This capability determines membership in the SONET interface group. This data is used by NNM iSPI Performance for Metrics.
com.hp.nnm.capability.iface.ietf.SONET-PATH	SDH Interface Metrics	Interface that supports the SONET-PATH-MIB metrics. This data is used by NNM iSPI Performance for Metrics.

### NNMi Advanced. IPv6

Unique Key	Capability	Description
com.hp.nnm.capability.iface.ipv6.rfc2465	RFC2465-IPv6-Interface	<p>(NNMi Advanced.) Indicates the interface is an IPv6 interface, <i>discovered using only the RFC 2465 IPv6-MIB and <b>not</b> the standard RFC 2863 IF-MIB.</i></p> <p>A small number of IPv6 devices do not support the standard RFC 2863 IF-MIB for IPv6 interfaces. In this case, NNMi uses the <i>RFC</i></p>

<sup>1</sup>Provider Edge router. The Internet Service Provider's router that receives your data on the path to your data's final destination. The Customer Edge (CE) router in your network connects to this PE.

**NNMi Advanced. IPv6, continued**

Unique Key	Capability	Description
		<p>2465 IPv6-MIB. When this happens, note the following:</p> <ul style="list-style-type: none"> <li>• Interface index (<i>ifIndex</i>) and description (<i>ifDescr</i>) are set according to the RFC 2465 IPv6 MIB.</li> <li>• Interface type (<i>ifType</i>) is set to <i>Other</i> (no specific type is available).</li> <li>• Interface Name (<i>ifName</i>), Alias (<i>ifAlias</i>), and Speed (<i>ifSpeed</i>) are blank (not available).</li> <li>• NNMi monitors the Status of this interface, but Performance metrics are not available.</li> </ul> <p>When an IP Address has the Interface Name (<i>ifName</i>) attribute set to blank, NNMi constructs an alternate string for the IP Address's <b>In Interface</b> attribute (<i>Other [&lt;ifIndex_value&gt;]</i>).</p>

NNMi Advanced. The capabilities in the following table identify how the interface is participating in a [Link Aggregation](#)<sup>1</sup>.

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

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

Unique Key	Capability	Description
<code>com.hp.nnm.capability.lag.aggregator</code>	Aggregator Interface	Indicates the interface represents a collection of participating interfaces at one end of an Aggregator Layer 2 Connection.  See <a href="#">Layer 2 Neighbor View Map Objects</a> for more information.
<code>com.hp.nnm.capability.lag.member</code>	Aggregation Member	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 when [Link Aggregation](#)<sup>1</sup> protocol is available.

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

Unique Key	Capability	Description
<code>com.hp.nnm.capability.lag.protocol.lacp</code>	802.3ad Link Aggregation Control Protocol	Indicates an interface using the IEEE 802.3ad Link Aggregation Control protocol (LACP).
<code>com.hp.nnm.capability.lag.protocol.static</code>	Static/Manual Configured Link Aggregation	Indicates the device has been configured with Static/Manual Configured Link Aggregation (static).
<code>com.hp.nnm.capability.lag.protocol.pagp</code>	Cisco Port	Cisco Systems

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

### NNMi Advanced. Link Aggregation Interface Capabilities: Protocols , continued

Unique Key	Capability	Description
	Aggregation Protocol	Port Aggregation Protocol (pagp)
<code>com.hp.nnm.capability.lag.protocol.mlt</code>	Nortel Multi-Link Trunking	Nortel Multi-Link Trunk technology (mlt)
<code>com.hp.nnm.capability.lag.protocol.istmlt</code>	Inter-Switch Trunk MLT	Split Multi-Link Trunk: inter-switch trunk (istMlt)
<code>com.hp.nnm.capability.lag.protocol.smlt</code>	Split MLT	Split Multi-Link Trunk: configuration technology (splitMlt)
<code>com.hp.nnm.capability.lag.protocol.unknown</code>	Unknown Protocol Link Aggregation	Indicates the hosting interface is a member of Link Aggregation with unknown protocol.

## Interface Capability Form

This form describes a capability added to the interface object by NNMi or an external application. Capabilities enable NNMi and application programmers to provide more information about a card than what is initially stored in the NNMi database.

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.

(*NNMi Advanced - Global Network Management feature*) Any Capability values added by an NNM iSPI are available on the Global Manager only if that iSPI is also running on the Global Manager.

### Interface Capability Attributes

Attribute	Description
Capability	Label used to identify the Capability that was added to the interface object.  "Interface Form: Capabilities Tab" on page 102 shows a list of all available Capabilities for that interface.

### Interface Capability Attributes, continued

Attribute	Description
	For more information, see <a href="#">"Interface Capabilities Provided by NNMI"</a> on page 103.
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> .  For more information, see <a href="#">"Interface Capabilities Provided by NNMI"</a> on page 103.

## 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 permits, you can edit a Custom Attribute. Only users assigned to the NNMI Administrator role can add a Custom Attribute.

*(NNMI Advanced - Global Network Management feature)* Custom Attribute values are not sent from a Regional Manager (NNMI management server) to the Global Manager. NNMI administrators for the Global Manager can configure Custom Attribute values that are stored in the NNMI database on the Global Manager.

### 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 Custom Attributes Form"</a> below.

## 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.

*(NNMI Advanced - Global Network Management feature)* Custom Attribute values are not sent from a Regional Manager (NNMI management server) to the Global Manager. NNMI administrators for the Global Manager can configure Custom Attribute values that are stored in the NNMI database on the Global Manager.

### 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 90 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.  Double-click the row representing an Interface Group. The "Interface Group Form" on page 232 displays all details about the selected Interface Group.

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






The "Interface Form" on page 90 provides details about the selected network interface.

**Tip:** This information is also visible in the Monitoring workspace, Interface Performance view.







**For information about each tab:**

The Performance tab displays data if the HP Network Node Manager iSPI Performance for Metrics Software software is installed and configured within your environment.

The icons on the Performance tab indicate the value from the most recent polling interval for interface performance states:

 <b>High</b> - The High threshold was crossed.	 <b>Abnormal Range</b> - This interface is abnormal based on the computed baseline for the specified threshold.
 <b>Nominal</b> - Measured within healthy range. (Or no thresholds are	 <b>Agent Error</b> - The SNMP agent responded with an error, rather than a value.
	 <b>Not Polled</b> - 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.



<p>being monitored.)</p> <p> <b>Low</b> - The Low threshold was crossed.</p> <p> <b>None</b> - The value returned was zero.</p>	<p> <b>No Polling Policy</b> - No performance polling policy exists for this measurement.</p> <p> <b>Normal Range</b> - This interface is normal based on the computed baseline for the specified threshold.</p> <p> <b>Unavailable</b> - State Poller is unable to compute the performance state or the computed value is outside of the valid range (for example: <math>\text{f}0.00 - 100.00</math>).</p> <p> <b>Unset</b> - An error condition exists, preventing successful measurement collection.</p>
---	--

**Tip:** NNMi can generate incidents based on threshold results

*Optional:* The NNMi administrator can configure thresholds for the metrics described in the following list. If you want to see the threshold configuration settings for the currently selected Interface, click **Actions** → **Configuration Details** → **Monitoring Settings**, then scroll down to the Count-Based Threshold Settings table and Time-Based Threshold Settings table:

- FCS LAN Error Rate

*Local Area Network interfaces only.* Threshold based on the percentage of incoming frames with a bad checksum (CRC value) compared to the total number of incoming frames. Possible causes include collisions at half-duplex, a duplex mismatch, bad hardware (NIC, cable, or port), or a connected device generating frames with bad Frame Check Sequence.

- FCS WLAN Error Rate

*Wireless Local Area Network Interfaces only.* Threshold based on the percentage of incoming frames with a bad checksum (CRC value) compared to the total number of incoming frames. Possible causes include wireless communication interference, bad hardware (NIC, cable or port), or a connected device generating frames with bad Frame Check Sequence.

- Input Discard Rate

Threshold based on the percentage of the interface's discarded input packet count compared to the total number of packets received. Packets might be discarded because of a variety of issues, including receive-buffer overflows, congestion, or system specific issues.

- Input Error Rate

Threshold based on the percentage of the interface's input packet error count compared to the total number of packets received. What constitutes an error is system specific, but likely includes such issues as bad packet checksums, incorrect header information, and packets that are too small.

- Input Queue Drops Rate

Threshold based on the percentage of the interface's dropped input packets compared to the total number of packets received. Possible causes include the input queue being full.

- Input Utilization

Threshold based on the percentage of the interface's total incoming octets compared to the maximum number of octets possible (determined by the MIB being used to query `ifSpeed` of

the device and whether the host system supports high-speed counters for interfaces).

**Tip:** Sometimes the `ifSpeed` value returned by the device's SNMP agent is not accurate and causes problems with thresholds. If your NNMi role allows, you can override the `ifSpeed` reported by the SNMP agent:

- a. Open the problem interface's Interface form.
- b. Select the [General Tab](#).
- c. Locate the Input/Output Speed section.
- d. Change the Input Speed or Output Speed setting.

- Output Discard Rate

Threshold based on the percentage of the interface's discarded output packet count compared to the total number of outgoing packets. Packets might be discarded because of a variety of issues, including transmission buffer overflows, congestion, or system specific issues.

- Output Error Rate

Threshold based on the percentage of the interface's output packet error count compared to the total number of outgoing packets. What constitutes an error is system specific, but likely includes such issues as collisions and buffer errors.

- Output Queue Drops Rate

Threshold based on the percentage of the interface's dropped output packets compared to the total number of outgoing packets. Possible causes include all buffers allocated to the interface being full.

- Output Utilization

Threshold based on the percentage of the interface's total outgoing octets compared to the maximum number of octets possible (determined by the MIB being used to query `ifSpeed` of the device and whether the host system supports high-speed counters for interfaces).

**Tip:** Sometimes the `ifSpeed` value returned by the device's SNMP agent is not accurate and causes problems with thresholds. If your NNMi role allows, you can override the `ifSpeed` reported by the SNMP agent:

- a. Open the problem interface's Interface form.
- b. Select the [General Tab](#).
- c. Locate the Input/Output Speed section.
- d. Change the Input Speed or Output Speed setting.

## Interface Form: Incidents Tab

The "Interface Form" on page 90 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>Double-click the row representing an incident. The "Incident Form" on page 311 displays all details about the selected incident.</p>

## Interface Form: Status Tab

The "Interface Form" on page 90 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> <p><b>Note:</b> The icons are displayed only in table views.</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 <code>ifAdminStatus</code> and <code>IfOperStatus</code>, as well as any conclusions. For information about how the current status was determined, see the "Interface Form: Conclusions Tab" on the next page. Status reflects the most serious outstanding conclusion. See "Watch Status Colors" on page 285 for more information about possible status values.</p>

### Status Tab, continued

Attribute	Description
	<i>NNMi Advanced</i> . <a href="#">Link Aggregation</a> <sup>1</sup> : If the Interface is an Aggregator, the Status is calculated using the combined Status of all Aggregation Member Interfaces. For more information, see "Interface Form: Link Aggregation Tab (NNMi Advanced)" on page 98 and <a href="#">Status Color for Link Aggregation Objects</a> .
Status Last Modified	Date and time indicating when the status was last set.

### Status History Table

Attribute	Description
Status History	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.  Double-click the row representing a Status History. The Status History form displays all details about the selected Status.

## Interface Form: Conclusions Tab

The "Interface Form" on page 90 provides details about the selected network interface.

All relevant conclusions are shown in the table on this tab. The most severe Status in the current group of conclusions becomes the overall Interface status. Some Interface conclusions propagate to other object types:

**For information about each tab:**

### Outstanding Status Conclusion Values

Attribute	Description
Outstanding Status Conclusions	The dynamically generated list of summary statuses of the interface that contributed to the current overall status of the selected interface. Status is set by the Causal Engine.  Each Conclusion listed is still outstanding and applies to the current overall Status.

---

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

### Outstanding Status Conclusion Values, continued

Attribute	Description																				
	<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 interface's most current Status.</p> <p>The Status value is correlated based on the most critical Conclusions.</p> <p>Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion.</p> <p>The following table describes the possible Conclusions that might appear for an interface object.</p> <div style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p><b>Note:</b> A <b>Y</b> in the <b>Incident?</b> column indicates that the Conclusion results in an incident.</p> </div> <p><b>Critical Status Conclusions</b></p> <table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>AggregatorDown</td> <td><b>Link Aggregation</b><sup>1</sup>: The Operational State of the Aggregator Interface is Down (if monitored), or all of the Aggregation Member Interfaces are Down. For more information, see "Interface Form: Link Aggregation Tab (NNMi Advanced)" on page 98.</td> <td>Critical</td> <td>Y</td> </tr> <tr> <td>InterfaceDown</td> <td>The interface Operational State is Down.</td> <td>Critical</td> <td>Y</td> </tr> </tbody> </table> <p><b>Major Status Conclusions NNM iSPI Performance for Metrics</b></p> <table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>InterfaceFCSELANErrorRateHigh</td> <td><i>Local Area Network.</i> Indicates a Frame Check Sequence (FCS) error rate on the</td> <td>Major</td> <td>Y</td> </tr> </tbody> </table>	Conclusion	Description	Status	Incident?	AggregatorDown	<b>Link Aggregation</b> <sup>1</sup> : The Operational State of the Aggregator Interface is Down (if monitored), or all of the Aggregation Member Interfaces are Down. For more information, see "Interface Form: Link Aggregation Tab (NNMi Advanced)" on page 98.	Critical	Y	InterfaceDown	The interface Operational State is Down.	Critical	Y	Conclusion	Description	Status	Incident?	InterfaceFCSELANErrorRateHigh	<i>Local Area Network.</i> Indicates a Frame Check Sequence (FCS) error rate on the	Major	Y
Conclusion	Description	Status	Incident?																		
AggregatorDown	<b>Link Aggregation</b> <sup>1</sup> : The Operational State of the Aggregator Interface is Down (if monitored), or all of the Aggregation Member Interfaces are Down. For more information, see "Interface Form: Link Aggregation Tab (NNMi Advanced)" on page 98.	Critical	Y																		
InterfaceDown	The interface Operational State is Down.	Critical	Y																		
Conclusion	Description	Status	Incident?																		
InterfaceFCSELANErrorRateHigh	<i>Local Area Network.</i> Indicates a Frame Check Sequence (FCS) error rate on the	Major	Y																		

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		interface has gone above a threshold setting.  The error rate is based on the number of frames that were received with a bad checksum (CRC value). Possible causes include collisions at half-duplex, a duplex mismatch, bad hardware (NIC, cable, or port), or a connected device generating frames with bad FCS.		
	InterfaceFCSWLANErrorRateHigh	<i>Wireless Local Area Network.</i> A Frame Check Sequence (FCS) error rate on the interface has gone above a threshold setting.  The error rate is based on the number of frames that were received with a bad checksum (CRC value). Possible causes include collisions at half-duplex, a duplex mismatch, bad hardware (NIC,	Major	Y

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		cable, or port), or a connected device generating frames with bad FCS.		
	InterfaceInputDiscardRateHigh	<p>The input discard rate on the interface has exceeded a threshold setting.</p> <p>This rate is based on the reported change in the number of input packets on the interface and the discarded packet count.</p>	Major	Y
	InterfaceInputErrorRateHigh	<p>The input error rate on the interface has exceeded a threshold setting.</p> <p>This rate is based on the reported change in the number of input packets on the interface and the packet error count.</p>	Major	Y
InterfaceInputQueueDropsRateHigh	<p>The number of input queue drops on the interface has exceeded a threshold setting.</p> <p>This range is based on the number of</p>	Major	Y	

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		<p>packets dropped because of a full queue. Possible causes include that the number of packet buffers allocated to the interface is exhausted or has reached its maximum threshold.</p>		
	InterfaceInputUtilizationHigh	<p>The input utilization on the interface has exceeded a threshold setting.</p> <p>This percentage is based on the interface speed and the reported change in the number of input bytes on the interface.</p>	Major	Y
	InterfaceInputUtilizationLow	<p>The input utilization on the interface is below a threshold setting.</p> <p>This percentage is based on the interface speed and the reported change in the number of input bytes on the interface.</p>	Major	Y
	InterfaceInputUtilizationNone	<p>The input utilization for the interface is zero</p>	Major	Y



**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		(0).  This value is based on the interface speed and the reported change in the number of input bytes on the interface.		
	InterfaceOutputDiscardRateHigh	The output discard rate on the interface has exceeded a threshold setting.  This rate is based on the reported change in the number of input packets on the interface and the discarded packet count.	Major	Y
	InterfaceOutputErrorRateHigh	The output error rate on the interface has exceeded a threshold setting.  This rate is based on the reported change in the number of output packets on the interface and the packet error count.	Major	Y
	InterfaceOutputQueueDropsRateHigh	The number of output queue drops on the interface has exceeded a	Major	Y

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		threshold setting.  This number is based on the number of packets dropped because of a full queue.		
	InterfaceOutputUtilizationHigh	The output utilization on the interface has exceeded a threshold setting.  This percentage is based on the interface speed and the reported change in the number of output bytes on the interface.	Major	Y
	InterfaceOutputUtilizationLow	The output utilization on the interface is below a threshold setting.  This percentage is based on the interface speed and the reported change in the number of output bytes on the interface.	Major	Y
	InterfaceOutputUtilizationNone	The output utilization on the interface is zero (0).  This value is based on the	Major	Y

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
		interface speed and the reported change in the number of output bytes on the interface.		
	<b>Minor Status Conclusions</b>			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
	AggregatorDegraded	<a href="#">Link Aggregation</a> <sup>1</sup> : One or more (but not all) Aggregation Member Interfaces that are part of the Aggregator Interface have an Operational State of Down. For more information, see " <a href="#">Interface Form: Link Aggregation Tab (NNMi Advanced)</a> " on page 98.	Minor	Y
	<b>Warning Status Conclusions</b> NNM iSPI Performance for Metrics			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
	InterfaceInputUtilizationAbnormal	The input utilization on the interface is abnormal based on the computed baseline.  This range is based on the interface speed and the reported change in the number of input	Warning	Y

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
		bytes on the interface.		
	InterfaceOutputUtilizationAbnormal	The output utilization on the interface is abnormal based on the computed baseline.  This range is based on the interface speed, and the reported change in the number of output bytes on the interface.	Warning	Y
	<b>Disabled Status Conclusions</b>			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
	InterfaceDisabled	The interface has been explicitly disabled by the device administrator.	Disabled	Y
	<b>Normal Status Conclusions</b>			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
	AggregatorUp	<a href="#">Link Aggregation</a> 1: The Aggregator	Normal	N

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		Interface and all Aggregation Member Interfaces have an Operational State of Up. For more information, see "Interface Form: Link Aggregation Tab (NNMi Advanced)" on page 98.		
	InterfaceEnabled	The interface has an Administrative State of Up.	Normal	N
	InterfaceFCSLANErrorRateInRange	<i>(NNMi SPI Performance for Metrics)</i> The Frame Check Sequence error rate for the interface is within the allowable range set by the administrator.	Normal	N
	InterfaceFCSWANErrorRateInRange	<i>(NNMi SPI Performance for Metrics)</i> The Frame Check Sequence error rate for the interface	Normal	N

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		is within the allowable range set by the administrator.		
	InterfaceInputDiscardRateLow	(NNM iSPI Performance for Metrics) The input discard rate for the interface is below the allowable low range set by the administrator.	Normal	N
	InterfaceInputDiscardRateNominal	(NNM iSPI Performance for Metrics) The input discard rate for the interface is within the allowable threshold range set by the administrator.	Normal	N
	InterfaceInputDiscardRateNone	(NNM iSPI Performance for Metrics) The input discard rate for the interface is zero (0) .	Normal	N
InterfaceInputErrorRateLow	(NNM iSPI Performance	Normal	N	

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		<i>for Metrics)</i> The input error rate for the interface is below the allowable threshold range set by the administrator.		
	InterfaceInputErrorRateNominal	<i>(NNM iSPI Performance for Metrics)</i> The input error rate for the interface is within the allowable threshold range set by the administrator.	Normal	N
	InterfaceInputErrorRateNone	<i>(NNM iSPI Performance for Metrics)</i> The input error rate for the interface is zero (0).	Normal	N
	InterfaceInputQueueDropsRateInRange	<i>(NNM iSPI Performance for Metrics)</i> The number of input queue drops for the interface is within the allowable range set by the administrator.	Normal	N

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
	InterfaceInputUtilizationNominal	<i>(NNM iSPI Performance for Metrics)</i> The input utilization for the interface is within the allowable threshold range set by the administrator.	Normal	N
	InterfaceInputUtilizationNormal	<i>(NNM iSPI Performance for Metrics)</i> The input utilization on the interface is normal based on the computed baseline. This range is based on the interface speed and the reported change in the number of input bytes on the interface.	Normal	N
	InterfaceOutputDiscardRateLow	<i>(NNM iSPI Performance for Metrics)</i> The output discard rate for the interface is below the allowable threshold	Normal	N



**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		range set by the administrator.		
	InterfaceOutputDiscardRateNominal	<i>(NNM iSPI Performance for Metrics)</i> The output discard rate for the interface is within the allowable threshold range set by the administrator.	Normal	N
	InterfaceOutputDiscardRateNone	<i>(NNM iSPI Performance for Metrics)</i> The output discard rate for the interface is zero (0).	Normal	N
	InterfaceOutputErrorRateLow	<i>(NNM iSPI Performance for Metrics)</i> The output error rate for the interface is below the allowable low range set by the administrator.	Normal	N
InterfaceOutputErrorRateNominal	<i>(NNM iSPI Performance for Metrics)</i> The output error rate for	Normal	N	

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		the interface is within the allowable threshold range set by the administrator.		
	InterfaceOutputErrorRateNone	<i>(NNM iSPI Performance for Metrics)</i> The output error rate for the interface is zero (0).	Normal	N
	InterfaceOutputQueueDropsRateInRange	<i>(NNM iSPI Performance for Metrics)</i> The number of output queue drops for the interface is within the allowable threshold range set by the administrator.	Normal	N
InterfaceOutputUtilizationNominal	<i>(NNM iSPI Performance for Metrics)</i> The output utilization for the interface is within the allowable threshold range set by the administrator.	Normal	N	

### Outstanding Status Conclusion Values, continued

Attribute	Description			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
	InterfaceOutUtilizationNormal	(NNMiSPI Performance for Metrics) The output utilization for the interface is within the allowable threshold range set by the administrator.	Normal	N
	InterfaceUp	The Operational State of the interface is Up.	Normal	N

## Interface Form: Registration Tab

The "Interface Form" on page 90 provides details about the selected network interface.

For information about each tab:

### Registration Attributes

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

### Object Identifiers Attributes

Attribute	Description
ID	The Unique Object Identifier, which is unique within the NNMi database.
UUID	The Universally Unique Object Identifier, which is unique across all databases.

## 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 permits, 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.
Mapped Address	If <i>static</i> Network Address Translation (NAT) is part of your network management domain, your NNMi administrator can configure NNMi to display the NAT <i>internal IP address</i> (such as private IPv4 address) assigned to the selected <i>external IP address</i> .
Status	Overall status for the current IP address. NNMi follows the ISO standard for status classification. See " <a href="#">IP Address Form: Status Tab</a> " on page 137.
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 in 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> .  ( <i>NNMi Advanced - Global Network Management feature</i> ) Any change to this Management Mode setting is sent from a Regional Manager to the Global Manager during the next Spiral Discovery cycle on the Regional Manager.  <b>Note:</b> If the NNMi Security configuration permits, you can change this setting using <b>Actions</b> → <b>Management Mode</b> .  <b>Tip:</b> You can right-click any object in a table or map view to access the <b>Actions</b> menu.
Direct Management	This attribute is set by the administrator and specifies whether an address should be managed or is temporarily out of service. Possible values are:

**Basic Attributes, continued**

Attribute	Description
Mode	<p> <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 in which it resides.</p> <p> <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.</p> <p> <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.</p> <p>This attribute is useful for notifying NNMi when an address is been temporarily out of service, or should never be managed.</p> <p><b>Note:</b> If you change the Direct Management Mode using <b>Actions</b> → <b>Management Mode</b>, 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>
State	<p>Indicates whether NNMi is communicating with the IP address. Possible values are:</p> <p> <b>Responding</b> – Indicates that the IP address is being polled and is responding to an ICMP ping.</p> <p> <b>Not Responding</b> – Indicates that the IP address is being polled, but is not responding to an ICMP ping.</p> <p>The following values indicate NNMi encountered trouble while trying to gather the required data:</p> <p> <b>No Polling Policy</b> - No polling policy exists in Monitoring Configuration settings for this monitored attribute.</p> <p> <b>Not Polled</b> - Indicates that this attribute is intentionally not polled, based on current Monitoring Configuration settings, current Communication Configuration settings, current polling policies, or because the parent Node is set to Not Managed or Out of Service</p> <p> <b>Unavailable</b> - Unable to determine the State. For example, the SNMP agent returned a value outside the range of possible values or returned a null value.</p> <p> <b>Unset</b> – Currently not used by NNMi.</p> <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	<p>The date and time when the State value was last modified.</p>

### Basic Attributes, continued

Attribute	Description
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	node in 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).  Click the  Lookup icon and select  Show Analysis or  Open to display more information about the node.
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	<i>(NNMi Advanced - Global Network Management feature)</i> The text you enter here is not sent from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager can add notes that are stored in the NNMi database on the Global Manager.  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.  Type a maximum of 1024 characters. Alpha-numeric, spaces, and special characters (~ ! @ # \$ % ^ & * ( ) _ + -) are permitted.  <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.

## IP Address Form: Incidents Tab

**Tip:** See "Incident Form" on page 311 for more details about the incident attributes that appear in the incident view's column headings.

The "IP Address Form" on page 132 provides details about the selected IP address.

**For information about each tab:**

### Incidents Table

Description
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.  Double-click the row representing an incident. The "Incident Form" on page 311 displays all details about the selected incident.

## IP Address Form: Capabilities Tab

The "IP Address Form" on page 132 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. Capabilities enable NNMi and application programmers to provide more information about an IP address than is initially stored in the NNMi database.

For example, NNMi uses the capability feature to identify an IPv4 [Anycast Rendezvous Point IP Address](#)<sup>1</sup> or IPv6 Anycast address so it is not polled. NNMi assigns the following capability to the address: `com.hp.nnm.capability.address.anycast`.

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

(*NNMi Advanced - Global Network Management feature*) Any Capability values added by an NNM iSPI are available on the Global Manager only if that iSPI is also running on the Global Manager.

### Capabilities Table

Attribute	Description
Capability	<p>Table of all of the capabilities associated with the selected IP Address. Use this table to access information about each Capability.</p> <p>Double-click the row representing a Capability. The "IP Address Capability Form" on page 137 displays all details about the selected Capability.</p> <p>For more information, see "IP Address Capabilities Provided by NNMi" below.</p>

## IP Address Capabilities Provided by NNMi

The "IP Address Form: Capabilities Tab" above displays a table of any capabilities added to a particular IP Address object. Capabilities enable NNMi and application programmers to provide more information about an IP address than what is initially stored in the NNMi database.

External applications can also add capabilities.

**KEY:** `com.hp.<product>.capability.<content>.<vendor/org>.<MIB/feature>`

Any Capability provided by NNMi begins with the prefix `com.hp.nnm.capability`.

`<product>` = Either NNMi or the NNM iSPI providing this capability.

---

<sup>1</sup>Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

<content> = card, ipaddr (address), iface (interface), lag ([Link Aggregation](#)<sup>1</sup> interface), node, rp (Router Redundancy), or metric (Node Sensor, Component Health, Component and Device Metrics).

<vendor/org> = Standards organization or vendor defining the MIB or feature associated with the capability.

<MIB/feature> = What this capability measures.

**Note:** The following table shows a few examples of the Capabilities provided by NNMI.

### IP Address Capability Attribute Values

Unique Key	Capability	Description
com.hp.nnm.capability.address.loopback	LOOPBACK	Used to identify a <a href="#">loopback address</a> <sup>2</sup> .
com.hp.nnm.capability.address.anycast	ANYCAST	Used to identify an address that is either of the following: <ul style="list-style-type: none"> <li>• IPv4 <a href="#">Anycast Rendezvous Point IP Address</a><sup>3</sup> that are loopback addresses used for routers in multi-cast network configurations. These duplicate IP addresses are excluded from monitoring.</li> <li>• NNMI Advanced: IPv6 Anycast address.</li> </ul>

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

<sup>2</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 Number 24, softwareloopback from the IANA ifType-MIB.

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



### IP Address Capability Attribute Values, continued

Unique Key	Capability	Description
com.hp.nnm.capability.address.nat	NAT (network address translation)	Used to map one address space into another (network masquerading to protect private networks).

## IP Address Capability Form

This form describes a capability added to the IP address object by NNMi or an external application. Capabilities enable NNMi and application programmers to provide more information about an IP address than what is initially stored in the NNMi database.

For example, NNMi uses the capability feature to identify an IPv4 [Anycast Rendezvous Point IP Address](#)<sup>1</sup> or IPv6 Anycast address. To exclude these addresses from polling, NNMi assigns following capability to the address: `com.hp.nnm.capability.ipaddr.anycast`

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

(*NNMi Advanced - Global Network Management feature*) Any Capability values added by an NNM iSPI are available on the Global Manager only if that iSPI is also running on the Global Manager.

### IP Address Capability Attributes

Attribute	Description
Capability	Label used to identify the Capability that was added to the IP address object.  "IP Address Form: Capabilities Tab" on page 135 shows a list of all available Capabilities for that IP address.  For more information, see "IP Address Capabilities Provided by NNMi" on page 135.
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> .  For more information, see "IP Address Capabilities Provided by NNMi" on page 135.









## IP Address Form: Status Tab

The "IP Address Form" on page 132 provides details about the selected IP address .

**For information about each tab:**

<sup>1</sup>Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

### 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</a>" below. Status reflects the most serious outstanding conclusion. See "<a href="#">Watch Status Colors</a>" on page 285 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 Table

Attribute	Description
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>Double-click the row representing a Status History. The Status History form displays all details about the selected Status.</p>

## IP Address Form: Conclusions Tab

The "[IP Address Form](#)" on page 132 provides details about the selected IP address .

All relevant conclusions are shown in the table on this tab. The most severe Status in the current group of conclusions becomes the overall IP Address status. Some IP Address conclusions propagate to other object types:

**For information about each tab:**

## Outstanding Status Conclusion Values

Attribute	Description																
Outstanding Status Conclusions	<p>The dynamically generated list of summary statuses of the IP address 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 IP address that led up to the address' most current Status.</p> <p>The Status value is correlated based on the most critical Conclusions.</p> <p>Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion.</p> <p>The following table describes the possible Conclusions that might appear for an IP Address object.</p> <p><b>Note:</b> A <b>Y</b> in the <b>Incident?</b> column indicates that the Conclusion results in an incident.</p> <p><b>Critical Status Conclusions</b></p> <table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>AddressNotResponding</td> <td>The address is not responding to ICMP ping.</td> <td>Critical</td> <td>Y</td> </tr> </tbody> </table> <p><b>Normal Status Conclusions</b></p> <table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>AddressResponding</td> <td>The address responds to ICMP ping.</td> <td>Normal</td> <td>N</td> </tr> </tbody> </table>	Conclusion	Description	Status	Incident?	AddressNotResponding	The address is not responding to ICMP ping.	Critical	Y	Conclusion	Description	Status	Incident?	AddressResponding	The address responds to ICMP ping.	Normal	N
Conclusion	Description	Status	Incident?														
AddressNotResponding	The address is not responding to ICMP ping.	Critical	Y														
Conclusion	Description	Status	Incident?														
AddressResponding	The address responds to ICMP ping.	Normal	N														

## IP Address Form: Registration Tab

The "IP Address Form" on page 132 provides details about the selected IP address .

**For information about each tab:**

### Registration Attributes

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

### Object Identifiers Attributes

Attribute	Description
ID	The Unique Object Identifier, which is unique within the NNMi database.
UUID	The Universally Unique Object Identifier, which is unique across all databases.

## 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 SNMP agent. This name is the hostname of the node (as stored in the NNMi database). NNMi chooses the hostname of the parent node according to the criteria specified by your NNMi administrator.</p> <p>NNMi follows a set of rules to dynamically generate the value stored in the NNMi database for each Node's Hostname. Click here for details.</p> <ul style="list-style-type: none"><li>• If the Node supports SNMP, NNMi requests the Hostname using the IP Address of the associated SNMP agent (the Management Address attribute value on the Node form).</li></ul> <p>When the NNMi administrator chooses <b>Enable SNMP Address Rediscovery</b> <input checked="" type="checkbox"/> in the Communication Configuration:</p> <ul style="list-style-type: none"><li>▪ If the SNMP Agent does not respond, NNMi checks for another Management Address to request the Hostname, and the Hostname could change.</li><li>▪ If the SNMP Agent associated with the node changes, the Management Address and Hostname could change.</li></ul> <p>When the NNMi administrator disables <b>Enable SNMP Address Rediscovery</b> <input type="checkbox"/> in the Communication Configuration:</p> <ul style="list-style-type: none"><li>▪ If the SNMP Agent does not respond, NNMi uses the previously gathered Management Address attribute value to request the Hostname.</li><li>▪ If the SNMP Agent associated with the node changes, NNMi uses the previously gathered Management Address attribute value to request the Hostname.</li></ul> <ul style="list-style-type: none"><li>• If the Node does not support SNMP, no Management Address is available. NNMi requests a Hostname starting with the lowest IP</li></ul>

### Basic Attributes, continued

Attribute	Description
	<p>Address associated with the node (a Discovery Seed value or an IP address value gathered from a neighboring device). NNMi uses the first Hostname provided. The Hostname might change during a future discovery cycle.</p> <p><b>Note:</b> NNMi administrators can use NNMi property file settings to change the way NNMi determines Hostname values:</p> <ul style="list-style-type: none"><li>• <code>nms-topology.properties</code> file settings: If DNS is the source of the Node's Hostname, there are three choices. By default NNMi uses the exact Hostname from your network configuration. It is possible to change NNMi behavior to convert Hostnames to all uppercase or all lowercase. See the "Modifying NNMi Normalization Properties" section of the <i>HP Network Node Manager i Software Deployment Reference</i>, which is available at: <a href="http://h20230.www2.hp.com/selfsolve/manuals">http://h20230.www2.hp.com/selfsolve/manuals</a>.</li><li>• <code>nms-disco.properties</code> file settings: The Hostname is either requested from the Node's lowest loopback interface IP address that resolves to a Hostname or requested from the Node's designated Management Address (SNMP agent address). With either choice, when no IP address resolves to a Hostname, the IP address itself becomes the Hostname. See the "Maintaining NNMi" chapter of the <i>HP Network Node Manager i Software Deployment Reference</i>, which is available at: <a href="http://h20230.www2.hp.com/selfsolve/manuals">http://h20230.www2.hp.com/selfsolve/manuals</a>.</li></ul>
Management Address	<p>IP address NNMi uses to communicate with this SNMP agent.</p> <p>The NNMi administrator can specify an address (Communication Configurations workspace, Specific Node settings tab), or NNMi can dynamically select one. Click here for details.</p> <p><b>Note:</b> With NNMi Advanced, the NNMi administrator specifies whether NNMi prefers IPv4 or IPv6 addresses when selecting the Management Address. See <a href="#">Configure Default SNMP, Management Address, and ICMP Settings</a>.</p> <ol style="list-style-type: none"><li>1. NNMi ignores the following addresses when determining which Management Address is most appropriate:<ul style="list-style-type: none"><li>■ Any address of an administratively-down interface.</li><li>■ Any address that is virtual (for example, <a href="#">VRRP</a><sup>1</sup>).</li></ul></li></ol>

<sup>1</sup>Virtual Router Redundancy Protocol

### Basic Attributes, continued

Attribute	Description
	<ul style="list-style-type: none"><li>■ Any IPv4 <b>Anycast Rendezvous Point IP Address</b><sup>1</sup> or IPv6 Anycast address.</li><li>■ Any address in the reserved loopback network range. IPv4 uses 127/24 (127 . * . * . *) and IPv6 uses ::1.</li><li>■ Any <b>IPv6 link-local address</b><sup>2</sup>.</li></ul> <p>2. If the NNMi Administrator specifies Enable SNMP Address Rediscovery in Communication Configuration, NNMi prefers the last-known Management Address (if any).</p> <p>3. If the Management Address does not respond and the NNMi Administrator specifies Enable SNMP Address Rediscovery in Communication Configuration, NNMi uses the Communication Configuration settings for <i>Management Address Selection</i>. The NNMi Administrators chooses the order in which NNMi checks the following:</p> <ul style="list-style-type: none"><li>■ Seed IP / Management IP - If the NNMi Administrator configures a Seed, NNMi uses the Seed address (either a specified IP address or the DNS address associated with a specified hostname) only during initial Discovery. NNMi then requests the current Management Address (the address from which the node's SNMP Agent responds) and uses that IP address for all communication after initial discovery.</li><li>■ Lowest Loopback - If a node supports multiple <b>loopback address</b><sup>3</sup>, NNMi queries each loopback addresses, starting with the lowest number. NNMi uses the loopback address with the lowest number from which the SNMP agent responds (for example, 10.16.42.197 is a lower number than 10.16.197.42).</li></ul>

<sup>1</sup>Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

<sup>2</sup>A non-routable IPv6 unicast address only used for communication with other nodes on the same link (LAN or VLAN). Link local addresses cannot be used for communication that must be forwarded through a router. IPv6 auto-configuration automatically assigns a unique link local address in the fe80::/10 address space to each IPv6-enabled interface on a system.



<sup>3</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 Number 24, softwareloopback from the IANA ifType-MIB.

## Basic Attributes, continued

Attribute	Description
	<ul style="list-style-type: none"><li>■ Highest Loopback - If a node supports multiple <b>loopback address</b><sup>1</sup>, NNMi queries each loopback addresses, starting with the highest number. NNMi uses the loopback address with the highest number from which the SNMP agent responds.</li><li>■ Interface Matching - The NNMi Administrator chooses which interface MIB variable NNMi queries to detect changes. NNMi can use the following MIB-II attribute values: <code>ifIndex</code>, <code>ifName</code>, <code>ifDescr</code>, <code>ifAlias</code>, or a combination of these (<code>ifName</code> or <code>ifDescr</code>, <code>ifName</code> or <code>ifDescr</code> or <code>ifAlias</code>).</li></ul> <ol style="list-style-type: none"><li>4. If no response, NNMi queries any remaining IP addresses in the node's IP address inventory, starting with the lowest number. NNMi uses the address with the lowest number from which the SNMP agent responds.</li><li>5. If no response, NNMi checks for any Mapped Address configured for one of the currently known addresses (see the Mapped Address column in the Custom IP Addresses view).</li></ol> <div data-bbox="613 898 1370 1142" style="background-color: #f0f0f0; padding: 10px;"><p><b>Note:</b> The address represents a <i>static</i> Network Address Translation (NAT) pair's <i>external IP address</i> from the internal/external IP address pair. NNMi Administrators configure these pairs using the Overlapping IP Address Mapping form. NNMi uses this list of addresses starting with IPv4 from low to high, then IPv6 from low to high.</p></div> <ol style="list-style-type: none"><li>6. If no response, NNMi might be configured to repeat the sequence using SNMPv1, SNMPv2c, or SNMPv3 in the order specified by the NNMi administrator (Communication Configurations <i>SNMP Minimum Security Level</i> settings).</li><li>7. When all else fails, NNMi retains the last known Management Address (if any) and automatically changes the State of that SNMP Agent object to Critical.</li></ol> <p>This process is repeated during each Spiral Discovery cycle, and the Management Address can change. For example, NNMi's inventory of addresses for the node expands, or the current Management Address does not respond to SNMP queries due to network problems or node reconfiguration. The NNMi administrator can prevent changes to the management address using the Communication Configurations <i>Enable SNMP Address Rediscovery</i> or <i>Preferred Management Address</i> setting.</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 Number 24, softwareloopback from the IANA ifType-MIB.

**Basic Attributes, continued**









Attribute	Description
Protocol Version	Version of the SNMP protocol in use. NNMi supports versions SNMPv1, SNMPv2c, and SNMPv3.
Read Community String	<p>The <i>read community string</i> value that was discovered for the selected SNMP agent.</p> <p><b>Note:</b> The read community string is an SNMPv1 or SNMPv2c password. The actual read community string is only visible if you are assigned to the Administrator role.</p>
Agent Enabled	Indicates whether this SNMP agent is set up for SNMP communication in your network environment.
UDP Port	<p>User Datagram Protocol port configuration for this SNMP agent.</p> <p>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.</p>
SNMP Proxy Address	<p><i>Prerequisite:</i> The NNMi administrator must specify one or more SNMP Proxy Servers in the NNMi Communication Configuration settings.</p> <p>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 enables NNMi to manage these nodes in the same way as nodes that provide SNMP access directly.</p>
SNMP Proxy Port	<p><i>Prerequisite:</i> The NNMi administrator must specify one or more SNMP Proxy Servers in the NNMi Communication Configuration settings.</p> <p>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.</p>
SNMP Timeout	(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.
<b>SNMP Agent State Attributes</b>	
Agent SNMP 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> <p> <b>Normal</b> – Indicates that the agent responds to SNMP queries.</p> <p> <b>Not Responding</b> – Indicates that the SNMP agent does not</p>



**Basic Attributes, continued**

Attribute	Description
	<p>respond to SNMP queries.</p> <p> <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. The SNMP Agent's address might or might not have an associated polling policy.</p> <p> <b>No Polling Policy</b>– Indicates that this SNMP Agent's address is being polled, but no polling policy exists in any Monitoring Configuration settings for this monitored attribute.</p> <p> <b>Unset</b> – Currently not used by NNMi.</p> <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</a>" on the next page for more information.</p>
<p>Management Address ICMP State</p>	<p>Indicates whether NNMi is communicating with the management address. Possible values are:</p> <p> <b>Responding</b> – Indicates that the management address is being polled and is responding to an ICMP ping.</p> <p> <b>Not Responding</b> – Indicates that the management address is being polled, but is not responding to an ICMP ping.</p> <p>The following values indicate NNMi encountered trouble while trying to gather the required data:</p> <p> <b>No Polling Policy</b> - No polling policy exists in Monitoring Configuration settings for this monitored attribute.</p> <p> <b>Not Polled</b> - Indicates that this attribute is intentionally not polled, based on current Monitoring Configuration settings, current Communication Configuration settings, current polling policies, or because the parent Node is set to Not Managed or Out of Service</p> <p> <b>Unavailable</b> - Unable to determine the State. For example, the ICMP poll returned a value outside the range of possible values or returned a null value.</p> <p> <b>Unset</b> – Currently not used by NNMi.</p> <p><b>Note:</b> NNMi's State Poller determines the State. The current state contributes towards the status calculation for the SNMP Agent.</p> <p>See the "<a href="#">SNMP Agent Form: Status Tab</a>" on the next page tab for more information.</p>

**Basic Attributes, continued**









Attribute	Description
Management Address Response Time State	<p><b>Note: Enable Management Address ICMP Polling</b> must be selected. See "Interface Form: Performance Tab (NNM iSPI Performance for Metrics)" on page 112 for more information.</p> <p>Indicates the State of the ICMP response time between the management station and the selected node. Possible values are:</p> <ul style="list-style-type: none"> <li> <b>Unavailable</b> - Unable to determine the State. For example, the ICMP poll returned a value outside the range of possible values or returned a null value.</li> <li> <b>Nominal</b> - Indicates the ICMP response time was between 0 and the configured High Value.</li> <li> <b>High</b> - Indicates a higher than configured ICMP response time between the management station and the selected node.</li> </ul>
Management Address Response Time Baseline	<p>HP Network Node Manager iSPI Performance for Metrics Software only.</p> <p><b>Note: Enable Node Component Performance Polling</b> must be selected. See "Interface Form: Performance Tab (NNM iSPI Performance for Metrics)" on page 112 for more information.</p> <p>Indicates the ICMP response time between the management station and the selected node is abnormal based on the computed baseline. Possible values are:</p> <ul style="list-style-type: none"> <li> <b>Abnormal Range</b> – Indicates State Poller has collected values outside the normal range when compared to the baseline data collected for the management address response time.</li> <li> <b>Normal Range</b> - Indicates State Poller collected values within the normal range when compared to the baseline data collected for the management address response time.</li> </ul>
State Last Modified	The date and time when the State value was last modified.
Hosted On Node	<p>Node on which the SNMP Agent 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  Show Analysis or  Open to display more information about the node.</p>

## SNMP Agent Form: Status Tab

The "SNMP Agent Form" on page 140 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>" below. Status reflects the most serious outstanding conclusion.</p>
Status Last Modified	Date and time indicating when the Status was last set.

### Status History Table

Attribute	Description
Status History	<p>List of the last 30 changes in the status for the SNMP agent. This view is useful for obtaining a summary of the SNMP agent status so that you can better determine any patterns in behavior and activity.</p> <p>Double-click the row representing a Status History. The Status History form displays all details about the selected Status.</p>

## SNMP Agent Form: Conclusions Tab

The "SNMP Agent Form" on page 140 provides details about the SNMP Agent of the selected node or interface.

For information about each tab:

### Outstanding Status Conclusion Values

Attribute	Description
Outstandi	The dynamically generated list of summary statuses for the SNMP agent that

### Outstanding Status Conclusion Values, continued

Attribute	Description																								
ng Status Conclusions	<p>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 SNMP Agent in the node contributes to the current Status of the SNMP Agent.</p> <p>The Status value is correlated based on the most critical Conclusions.</p> <p>Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion.</p> <p>The following table describes the possible Conclusions that might appear for an SNMP Agent object.</p> <p><b>Note:</b> A Y in the <b>Incident?</b> column indicates that the Conclusion results in an incident.</p> <p><b>Critical Status Conclusions</b></p> <table border="1" data-bbox="435 877 1377 1096"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>SNMPAgentNotResponding</td> <td>The SNMP agent is not responding to SNMP queries on the selected node.</td> <td>Critical</td> <td>Y</td> </tr> </tbody> </table> <p><b>Minor Status Conclusions</b></p> <table border="1" data-bbox="435 1163 1377 1381"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>SNMPAgentPingNotResponding</td> <td>The address associated with this SNMP Agent is not responding to ping.</td> <td>Minor</td> <td>N</td> </tr> </tbody> </table> <p><b>Warning Status Conclusions</b></p> <table border="1" data-bbox="435 1449 1377 1852"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>ManagementAddressICMPResponseTimeAbnormal</td> <td>Indicates there is an abnormal Internet Control Message Protocol (ICMP)</td> <td>Warning</td> <td>Y</td> </tr> </tbody> </table>	Conclusion	Description	Status	Incident?	SNMPAgentNotResponding	The SNMP agent is not responding to SNMP queries on the selected node.	Critical	Y	Conclusion	Description	Status	Incident?	SNMPAgentPingNotResponding	The address associated with this SNMP Agent is not responding to ping.	Minor	N	Conclusion	Description	Status	Incident?	ManagementAddressICMPResponseTimeAbnormal	Indicates there is an abnormal Internet Control Message Protocol (ICMP)	Warning	Y
Conclusion	Description	Status	Incident?																						
SNMPAgentNotResponding	The SNMP agent is not responding to SNMP queries on the selected node.	Critical	Y																						
Conclusion	Description	Status	Incident?																						
SNMPAgentPingNotResponding	The address associated with this SNMP Agent is not responding to ping.	Minor	N																						
Conclusion	Description	Status	Incident?																						
ManagementAddressICMPResponseTimeAbnormal	Indicates there is an abnormal Internet Control Message Protocol (ICMP)	Warning	Y																						

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		<p>response time from the NNMi management server to the selected node.</p> <p>ICMP messages are typically used for diagnostic or routing purposes for determining whether a host or router could not be reached.</p> <p>The incident is generated when NNMi detects a higher or lower value than the baseline ICMP response time between the NNMi management server and the</p>		

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		selected node.		
	ManagementAddressICMPResponseTimeHigh	<p>Indicates a high Internet Control Message Protocol (ICMP) response time from the management station to the selected node.</p> <p>ICMP messages are typically used for diagnostic or routing purposes for determining whether a host or router could not be reached.</p> <p>The incident is generated when NNMi detects a higher than</p>	Warning	Y

**Outstanding Status Conclusion Values, continued**

Attribute	Description											
	<table border="1"> <thead> <tr> <th data-bbox="423 273 987 373">Conclusion</th> <th data-bbox="990 273 1146 373">Description</th> <th data-bbox="1149 273 1252 373">Status</th> <th data-bbox="1255 273 1385 373">Incident?</th> </tr> </thead> <tr> <td data-bbox="423 378 987 772"></td> <td data-bbox="990 378 1146 772">configured ICMP response time between the NNMi management server and the selected node.</td> <td data-bbox="1149 378 1252 772"></td> <td data-bbox="1255 378 1385 772"></td> </tr> </table>	Conclusion	Description	Status	Incident?		configured ICMP response time between the NNMi management server and the selected node.					
Conclusion	Description	Status	Incident?									
	configured ICMP response time between the NNMi management server and the selected node.											
	<b>Normal Status Conclusions</b>											
	<table border="1"> <thead> <tr> <th data-bbox="423 833 987 934">Conclusion</th> <th data-bbox="990 833 1146 934">Description</th> <th data-bbox="1149 833 1252 934">Status</th> <th data-bbox="1255 833 1385 934">Incident?</th> </tr> </thead> <tr> <td data-bbox="423 938 987 1843">ManagementAddressICMPResponseTimeNominal</td> <td data-bbox="990 938 1146 1843">Indicates that the Internet Control Message Protocol (ICMP) response time from the management station to the selected node is within the threshold range set by the administrator.  ICMP messages are typically used for diagnostic</td> <td data-bbox="1149 938 1252 1843">Normal</td> <td data-bbox="1255 938 1385 1843">N</td> </tr> </table>	Conclusion	Description	Status	Incident?	ManagementAddressICMPResponseTimeNominal	Indicates that the Internet Control Message Protocol (ICMP) response time from the management station to the selected node is within the threshold range set by the administrator.  ICMP messages are typically used for diagnostic	Normal	N			
Conclusion	Description	Status	Incident?									
ManagementAddressICMPResponseTimeNominal	Indicates that the Internet Control Message Protocol (ICMP) response time from the management station to the selected node is within the threshold range set by the administrator.  ICMP messages are typically used for diagnostic	Normal	N									

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		or routing purposes for determining whether a host or router could not be reached.		
	ManagementAddressICMPResponseTimeNormal	Indicates if Internet Control Message Protocol (ICMP) response time from the NNMi management server to the selected node is within the baseline set by the administrator. ICMP messages are typically used for diagnostic or routing purposes for determining whether a host or router could not be reached.	Normal	N



### Outstanding Status Conclusion Values, continued

Attribute	Description			
	Conclusion	Description	Status	Incident?
	SNMPAgentPingResponding	The address associated with this SNMP Agent is responding to ping.	Normal	N
	SNMPAgentResponding	The SNMP Agent is responding to SNMP requests.	Normal	N

## SNMP Agent Form: Incidents Tab

The "SNMP Agent Form" on page 140 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>Double-click the row representing an incident. The "Incident Form" on page 311 displays all details about the selected incident.</p>

## SNMP Agent Form: Registration Tab

The "SNMP Agent Form" on page 140 provides details about the SNMP Agent of the selected node or interface.

For information about each tab:

### Registration Attributes

Attribute	Description
Created	Date and time the selected object instance was created. NNMi uses the locale of the

**Registration Attributes, continued**

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

**Object Identifiers Attributes**

Attribute	Description
ID	The Unique Object Identifier, which is unique within the NNMi database.
UUID	The Universally Unique Object Identifier, which is unique across all databases.

## IP Subnet Form

The IP Subnet form provides details about the selected subnet. Each IP Subnet represents an IP Subnet within a particular Tenant (that IPv4 Subnet definition independently applies to each Tenant).

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

**For information about each tab:**

**Basic Attributes**

Attribute	Description
Name	Subnet in your 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.
Tenant	Tenants enable NNMi administrators to partition a network across multiple customers. The NNMi administrator controls the Tenant assignment for each Node.  A Tenant is the top-level organization to which a Node belongs.  Devices that belong to the Default Tenant can have Layer 2 Connections to any device in any Tenant. Devices within any Tenant <i>other than</i> Default Tenant can have Layer 2 Connections <i>only</i> to devices within the same Tenant or the Default Tenant.
Notes	<i>(NNMi Advanced - Global Network Management feature)</i> The text you enter here is not sent from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager can add notes that are stored in the NNMi database on the Global Manager.  Provided for network operators to use for any additional notes required to further

### Basic Attributes, continued

Attribute	Description
	<p>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.</p> <p>Type a maximum of 1024 characters. Alpha-numeric, spaces, and special characters (~ ! @ # \$ % ^ &amp; * ( ) _ + -) are permitted.</p> <p><b>Note:</b> You can sort your subnet table views based on this value. Therefore, you might want to include keywords for this attribute value.</p>

## IP Subnet Form: IP Addresses Tab

The "IP Subnet Form" on the [previous page](#) provides details about the selected subnet.

**For information about each tab:**

### IP Addresses Table

Attribute	Description
IP Addresses	<p>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.</p> <p>Double-click the row representing an IP address. The "IP Address Form" on <a href="#">page 132</a> displays all details about the selected IP address.</p>

## IP Subnet Form: Registration Tab

The "IP Subnet Form" on the [previous page](#) provides details about the subnet selected.

**For information about each tab:**

### Registration Attributes

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

### Object Identifiers Attributes

Attribute	Description
ID	The Unique Object Identifier, which is unique within the NNMi database.
UUID	The Universally Unique Object Identifier, which is unique across all databases.

## 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 the following:

- A trunk port can participate in multiple VLANs.
- Only the objects to which you have access are visible from the form.

### For information about each tab:

(*NNMi Advanced - Global Network Management feature*) There might be slight differences between the VLAN information shown on Regional Managers and Global Managers, because the VLAN calculations use [Layer 2 Connections](#) data.

The following attributes always appear on the VLAN form, whether you access that form from the VLAN view or from a VLAN Port form's tab.

### Basic Attributes

Attribute	Description
Global VLAN Name	<p>VLAN connections are determined by a common VLAN Id. The <i>name</i> assigned to that VLAN can be designated by each participating Node\Interface's configuration settings for that VLAN Id. Therefore, NNMi chooses a VLAN name for this value (from potentially many names for the same VLAN Id):</p> <p>Global VLAN Name = NNMi uses the lowest sort-order name from all available names designated by member Nodes.</p> <p><b>Tip:</b> If you see an attribute named <i>Local VLAN Name</i> = the VLAN name assigned by the configuration settings on the currently selected Node\Interface.</p>
VLAN Id	<p>The identification value for the current VLAN. This value is taken directly from the MIB file provided by the Vendor.</p>

The following attributes display only when displaying information about a row in the VLAN view.

### VLAN Statistics Attributes

Attribute	Description
Member Node [Interface]	<p><code>hostname[Interface Name]</code></p> <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><li>• The User Group to Security Group mapping enables the user to view the node.</li></ul>

### VLAN Statistics Attributes, continued

Attribute	Description
	NNMi selects the Member Interface using the following criteria: <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><li>• The User Group to Security Group mapping enables the user to view the node to which the interface belongs.</li></ul>
Member Node Count	Specifies the number of nodes that belong to the current VLAN.

#### Related Topics:

["VLANs View \(Inventory\)" on page 33](#)

## VLAN Form: Ports Tab

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

The "VLAN Form" on the previous page provides details about the selected VLAN.

#### Ports Associated with this VLAN

Attribute	Description
Ports	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.  Double-click the row representing a Port. The "Port Form" on page 171 displays all details about the selected Port.

#### Related Topics:

["VLANs View \(Inventory\)" on page 33](#)

## Card Form















The Card form provides details about the Card you selected on the Node form or Inventory: Cards view. The following table describes the fields included on Basics section of the Card form.

#### For information about each tab:




##### Basic Attributes

Attribute	Description
Name	The name of the card. Sometimes it's the descriptive string used by the network administrator to name the card. For example, SupIII1000SX, Ether10/100TX,

**Basic Attributes, continued**

Attribute	Description
	<p>RSM-Mod, and ATM-OC3-Phy.</p> <p>If the Name value is null, NNMi uses the card Index value (see below).</p>
Hosted on Node	<p>Node in which the card 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  Show Analysis or  Open to display more information about the node.</p>
Status	<p>Overall status for the current card. NNMi follows the ISO standard for status classification. See the "<a href="#">Card Form: Status Tab</a>" on page 167 for more information. 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> <li> Disabled</li> <li> Unknown</li> <li> No Status</li> </ul> <p>Card status is derived from SNMP polling results for <a href="#">Administrative State</a>, <a href="#">Operational State</a>, and the most serious outstanding conclusion. See the "<a href="#">Card Form: Conclusions Tab</a>" on page 169 for information about how the current status was determined. See "<a href="#">Watch Status Colors</a>" on page 285 for more information about possible status values.</p> <p><b>Note:</b> The icons are displayed only in table views.</p>
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</p>













### Basic Attributes, continued

Attribute	Description
	<p>of service, or should never be managed.</p> <p><i>(NNMi Advanced - Global Network Management feature)</i> Any change to this Management Mode setting is sent from a Regional Manager to the Global Manager during the next Spiral Discovery cycle on the Regional Manager.</p> <p><b>Note:</b> If the NNMi Security configuration permits, you can change this setting using <b>Actions</b> → <b>Management Mode</b>.</p> <p><b>Tip:</b> You can right-click any object in a table or map view to access the <b>Actions</b> menu.</p>
Direct Management Mode	<p>Indicates whether the current card is being managed. This attribute is set by the administrator and specifies whether a card should be managed or whether a card is temporarily out of service. Possible values are:</p> <ul style="list-style-type: none"> <li> <b>Inherited</b> – Used to indicate that the card should inherit the Management Mode from the node in which it resides.</li> <li> <b>Not Managed</b> – Used to indicate that NNMi does not discover or monitor the card.</li> <li> <b>Out of Service</b> – Used to indicate a card is unavailable because it is out of service. NNMi does not discover or monitor these cards.</li> </ul> <p>This attribute is useful for notifying NNMi when a card is temporarily out of service, or should never be managed.</p> <p><b>Note:</b> If you change the Direct Management Mode using <b>Actions</b> → <b>Management Mode</b>, 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 Card	If this card is plugged into another card, the Name of that card is listed here.
Redundant Group	Indicates whether this card participates in a group of cards that provide redundancy protection against processor card failure.

### Card State Attributes

















Attribute	Description
Administrative State	<p>Either the current card Administrative State value. The NNMi State Poller interprets and normalizes the State value returned for the monitored attribute to handle the differences between vendors. The current Administrative State contributes towards the status calculation for this card. See the "<a href="#">Card Form: Status Tab</a>" on page 167 for more information.</p>

### Card State Attributes, continued
















Attribute	Description
	<p><b>Note:</b> If the card's SNMP agent supports only the <a href="#">Internet Engineering Task Force (IETF) ENTITY-MIB</a>, no state or status information is available. NNMi sets this state to  <b>No Polling Policy</b> and the card status to  No Status. If you look on the parent <a href="#">"Node Form" on page 50</a>, you will see the <code>com.hp.nnm.capability.card.ietf.entity</code> capability in the list.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> <li> <b>Up</b> – The SNMP agent responded with a card administrative status value of Up.</li> <li> <b>Down</b> – The SNMP agent responded with a card administrative status value of Down.</li> <li> <b>Other</b> – The SNMP agent responded with a value for card administrative status that is not recognized.</li> </ul> <p>The following values indicate NNMi could not gather the required data:</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 this agent.</li> <li> <b>No Polling Policy</b> - Indicates the object is being polled, but no polling policy exists in Monitoring Configuration settings for this monitored attribute.</li> <li> <b>Not Polled</b> - Indicates that this 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. This object attribute might or might not have an associated polling policy.</li> <li> <b>Unavailable</b> - Unable to determine the State. For example, the SNMP agent returned a value outside the range of possible values or returned a null value.</li> <li> <b>Unset</b> – Currently not used by NNMi.</li> </ul>
Operational State	<p>The current card Operational State value. The NNMi State Poller interprets and normalizes the State value returned for the monitored attribute to handle the differences between vendors. The current Operational State contributes towards the status calculation for this card. See the <a href="#">"Card Form: Status Tab" on page 167</a> for more information.</p> <p><b>Note:</b> If the card's SNMP agent supports only the <a href="#">Internet Engineering Task Force (IETF) ENTITY-MIB</a>, no state or status information is available. NNMi sets this state to  <b>No Polling Policy</b> and the card status to  No Status. If you look on the parent <a href="#">"Node Form" on page 50</a>, you will see the <code>com.hp.nnm.capability.card.ietf.entity</code> capability in the list.</p> <p>Possible values are:</p>



**Card State Attributes, continued**

Attribute	Description
	<p> <b>Up</b> – The SNMP agent responded that the card is operationally up, ready to receive and send network traffic.</p> <p> <b>Disabled</b> – The card's <i>Administrative State</i> is set to  <b>Down</b>.</p> <p> <b>Down</b> – The SNMP agent responded that the card is operationally down.</p> <p> <b>Dormant</b> – Indicates the card is in a "pending" state, waiting for some external event.</p> <p> <b>Minor Fault</b> – Indicates that the card or one of its hardware components is experiencing a partial failure.</p> <p> <b>Not Present</b> – Indicates that the card module is not installed or is missing some hardware component.</p> <p> <b>Other</b> – The SNMP agent responded with a value for card operational status that is not recognized.</p> <p> <b>Testing</b> – The SNMP agent responded that the card is in test mode.</p> <p> <b>Transient</b> – Indicates the card is in a transient state. For example, rebooting.</p> <p> <b>Unknown</b> – The SNMP agent responded with a card operational status value of <i>unknown</i>.</p> <p>The following values indicate NNMi could not gather the required data:</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> - No polling policy exists in Monitoring Configuration settings for this monitored attribute.</p> <p> <b>Not Polled</b> - Indicates that this attribute is intentionally not polled, based on current Monitoring Configuration settings, current Communication Configuration settings, current polling policies, or because the parent Node is set to Not Managed or Out of Service</p> <p> <b>Unavailable</b> - The SNMP agent responded with a value for card operational status of <i>Not-Specified</i>, so NNMi is unable to determine the State. Other possibilities: the SNMP agent returned a value outside the range of possible values or returned a null value.</p> <p> <b>Unset</b> – Currently not used by NNMi.</p>
Current Standby State	<p>Either the current MIB-II <i>Standby State</i> value or a value the NNMi State Poller interprets and normalizes to handle differences between vendors. The current Standby State contributes towards the status calculation for this card. See the "<a href="#">Card Form: Status Tab</a>" on page 167 for more information.</p>

### Card State Attributes, continued

Attribute	Description
	<p><b>Note:</b> If the card's SNMP agent supports only the <a href="#">Internet Engineering Task Force (IETF) ENTITY-MIB</a>, no state or status information is available. NNMi sets this state to  <b>No Polling Policy</b> and the card status to  No Status. If you look on the parent "<a href="#">Node Form</a>" on page 50, you will see the <code>com.hp.nnm.capability.card.ietf.entity</code> capability in the list.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> <li> <b>Active</b> - Indicates the card is the active card in the Card Redundancy Group.</li> <li> <b>Cold-Standby</b> - Indicates the card is not in use, but is available to take over the role of the active card after it is initialized.</li> <li> <b>Hot-Standby</b> - Indicates the card is not in use, but can immediately take over the role of the active card.</li> <li> <b>Standby</b> - Indicates the card is a candidate to become the next active card.</li> <li> <b>Error</b> - Indicates the card cannot take over the role of active or standby card in the Card Redundancy Group.</li> <li> <b>Other</b> – The SNMP agent on the card responded with a value for Standby State of <b>Other</b> or one that is not recognized.</li> <li> <b>Transient</b> – Indicates the card is in a transient state. For example, rebooting.</li> <li> <b>Unknown</b> - Indicates the card is unable to report Standby State.</li> </ul> <p>The following values indicate NNMi could not gather the required data:</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 this agent.</li> <li> <b>No Polling Policy</b> - Indicates the object is being polled, but no polling policy exists in Monitoring Configuration settings for this monitored attribute.</li> <li> <b>Not Polled</b> - Indicates that this 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. This object attribute might or might not have an associated polling policy.</li> <li> <b>Unavailable</b> - Unable to determine the State. For example, the SNMP agent returned a value outside the range of possible values or returned a null value.</li> <li> <b>Unset</b> – Currently not used by NNMi.</li> </ul>
Previous	The Standby State that was determined before the current Standby State. See

### Card State Attributes, continued

Attribute	Description
Standby State	<a href="#">Standby State</a> for more information about Standby State and the possible values.
State Last Modified	The date and time when any combination of the Stand By State, Administrative State, and Operational State were last modified.

### Notes Attributes

Attribute	Description
Notes	<p>(<i>NNMi Advanced - Global Network Management feature</i>) The text you enter here is not sent from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager can add notes that are stored in the NNMi database on the Global Manager.</p> <p>Provided for network operators to use for any additional information about this card that you want to communicate to your team.</p> <p>Type a maximum of 1024 characters. Alpha-numeric, spaces, and special characters (~ ! @ # \$ % ^ &amp; * ( ) _ + -) are permitted.</p> <p><b>Note:</b> You can sort your Card table views based on this value. Therefore, you might want to include keywords for this attribute value.</p>

## Card Form: General Tab

The "Card Form" on page 157 provides details about the selected card.

For information about each tab:

### General Attributes

Attribute	Description
Model Name	Card model name or number designator, determined by the vendor.
Type	The hardware-type designator for the card, determined by the vendor. For example: <ul style="list-style-type: none"> <li>cevCat6kWsSup720Base</li> <li>wssup720base(1002)</li> <li>cat6k-ws-sup720-base</li> </ul>
Serial Number	Card serial number, determined by the vendor.
Firmware Version	The firmware version or revision for the card, determined by the vendor. For example, 5.4(2).
Hardware Version	The hardware version or revision for the card, determined by the vendor. For example, 3.1.

### General Attributes, continued

Attribute	Description
Software Version	The software version or revision for the card, determined by the vendor. For example, 12.2(33)SXI
Index	<p>The unique value assigned to each card within a chassis or another card. The value chosen is always consistent with the Name value assigned to the card's hosted port. For example, the index of card hosting port Fa5/1 is 5 and the index of card hosting port J8 is J.</p> <p>If ENTITY-MIB is the <i>only MIB</i> supported for a particular card, this attribute has the same value as the Physical Index attribute.</p>
Physical Index	NNMi gathers this attribute value if the ENTITY-MIB is supported by the card's vendor.
Description	<p>The description assigned to the card by the operating system of the device in which the card is mounted. Examples:</p> <ul style="list-style-type: none"><li>• WS-X5530 1000BaseSXSupervisor Rev. 1.8</li><li>• WS-X5225R 10/100BaseTX Ethernet Rev. 1.1</li><li>• HP J4111A 8-port 10/100Base-TX module</li></ul>

## Card Form: Ports Tab

The "Card Form" on page 157 provides details about the selected card.

**For information about each tab:**

### Ports Associated with this Card

Attribute	Description
Ports	<p>Table of all of the ports associated with the selected card. Use this table to access information about each port associated with the selected card.</p> <p>Double-click the row representing a Port. The "Port Form" on page 171 displays all details about the selected Port.</p>

## Card Form: Daughter Cards Tab

The "Card Form" on page 157 provides details about the selected card.

**For information about each tab:**

### Daughter Cards Attached to this Card

Attribute	Description
Daughter Cards	Table of all of the cards that are plugged into the selected card. Use this table to access information about each daughter card associated with the selected parent card.

### Daughter Cards Attached to this Card, continued

Attribute	Description
	Double-click the row representing a Card. The "Card Form" on page 157 displays all details about the selected Card.

## Card Form: Capabilities Tab

The "Card Form" on page 157 provides details about the selected card.

The Card Form: Capabilities tab displays a table of any capabilities added to the card object by NNMi or an external application. Capabilities enable NNMi and application programmers to provide more information about a card than is initially stored in the NNMi database.

### For information about each tab:

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

(*NNMi Advanced - Global Network Management feature*) Any Capability values added by an NNM iSPI are available on the Global Manager only if that iSPI is also running on the Global Manager.

### Capabilities of this Card

Attribute	Description
Capability	Table of all of the capabilities associated with the selected Card. Use this table to access information about each Capability.  Double-click the row representing a Capability. The "Card Capability Form" on the next page displays all details about the selected Capability.  For more information, see "Card Capabilities Provided by NNMi" below.

## Card Capabilities Provided by NNMi

The "Card Form: Capabilities Tab" above displays a table of any capabilities added to a particular card object. Capabilities enable NNMi and application programmers to provide more information about a card than what is initially stored in the NNMi database.

External applications can also add capabilities.

**KEY:** `com.hp.<product>.capability.<content>.<vendor/org>.<MIB/feature>`

Any Capability provided by NNMi begins with the prefix `com.hp.nnm.capability.`

`<product>` = Either NNMi or the NNM iSPI providing this capability.

<content> = card, ipaddr (address), iface (interface), lag ([Link Aggregation](#)<sup>1</sup> interface), node, rp (Router Redundancy), or metric (Node Sensor, Component Health, Component and Device Metrics).

<vendor/org> = Standards organization or vendor defining the MIB or feature associated with the capability.

<MIB/feature> = What this capability measures.

**Note:** The following table shows an example of the Capabilities provided by NNMi.

### Card Capability Attribute Values

Unique Key	Capability	Description
com.hp.nnm.capability.card.fru	Field Replaceable Unit	Indicates the device is a replaceable card (Field Replaceable Unit).

## Card Capability Form

This form describes a capability added to the card object by NNMi or an external application. Capabilities enable NNMi and application programmers to provide more information about a card than what is initially stored in the NNMi database.

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

(*NNMi Advanced - Global Network Management feature*) Any Capability values added by an NNM iSPI are available on the Global Manager only if that iSPI is also running on the Global Manager.

### Card Capability Attributes

Attribute	Description
Capability	Label used to identify the Capability that was added to the card object.  "Card Form: Capabilities Tab" on the previous page shows a list of all available Capabilities for that card.  For more information, see "Card Capabilities Provided by NNMi" on the previous page.
Unique	Used as a unique identifier for the Capability. Any capability provided by NNMi

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

### Card Capability Attributes, continued

Attribute	Description
Key	begins with the prefix <code>com.hp.nnm.capability</code> .  For more information, see "Card Capabilities Provided by NNMi" on page 165.

## Card Form: Incidents Tab

The "Card Form" on page 157 provides details about the selected card.

For information about each tab:

### Incidents Associated with this Card








Attribute	Description
Incidents	Table of the Incidents associated with the selected card.  These Incidents are sorted by creation time so that you can view the Incidents in chronological order. Use this table to determine which Incidents are still open for the selected card.  Double-click the row representing an incident. The "Incident Form" on page 311 displays all details about the selected incident.  <b>Tip:</b> See "Incident Form" on page 311 for more details about the incident attributes that appear in the incident table's column headings.

## Card Form: Status Tab


The "Card Form" on page 157 provides details about the selected card.

For information about each tab:

### Overall Status Attributes

Attribute	Description
Status	Overall status for the current card. NNMi follows the ISO standard for status classification. Possible values are: <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></ul>

**Overall Status Attributes, continued**

Attribute	Description
	<p> Critical</p> <p>Card status is derived from SNMP polling results for <a href="#">Administrative State</a>, <a href="#">Operational State</a>, and the most serious outstanding conclusion. See the "<a href="#">Card Form: Conclusions Tab</a>" on the next page for information about how the current status was determined. See "<a href="#">Watch Status Colors</a>" on page 285 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.








**Card Status History Table**

Attribute	Description
Status History	<p>Table of up to the last 30 changes in the status for the Card. This table is useful for obtaining a summary of the Card Status so that you can better determine any patterns in behavior and activity.</p> <p>Double-click the row representing a Status History. The "<a href="#">Card Status History Form</a>" below displays all details about the selected Status.</p>

**Card Status History Form**

Card status is derived from SNMP polling results for [Administrative State](#), [Operational State](#), and the most serious outstanding conclusion. See the "[Card Form: Conclusions Tab](#)" on the next page for information about how the current status was determined. See "[Watch Status Colors](#)" on page 285 for more information about possible status values.

**Status Attributes**

Attribute	Description
Status	<p>Overall status for the current card. 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> </ul>



### Status Attributes, continued

Attribute	Description
	<p>✖ Critical</p> <p>Card status is derived from SNMP polling results for <a href="#">Administrative State</a>, <a href="#">Operational State</a>, and the most serious outstanding conclusion.</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.

## Card Form: Conclusions Tab

The "Card Form" on page 157 provides details about the selected card.

For information about each tab:

### Outstanding Status Conclusion Values

Attribute	Description
Outstanding Status Conclusions	<p>The table of dynamically generated summary statuses for the card that contributed to the current overall Status of the selected card. Status is set by the <a href="#">Causal Engine</a><sup>1</sup>.</p> <p>Each Conclusion listed is outstanding and contributes to the current overall Status.</p> <p>This table is useful for obtaining a quick summary of the problem description for the current card that led up to the card's most current Status.</p> <p>Card Status is derived from the most serious outstanding Conclusion and SNMP polling results for <a href="#">Administrative State</a> and <a href="#">Operational State</a>.</p> <p>Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion.</p> <p>The following table describes the possible Conclusions that might appear for a Card object.</p> <p><b>Note:</b> A Y in the <b>Incident?</b> column indicates that the Conclusion results in an incident.</p> <p><b>Critical Status Conclusions</b></p>

<sup>1</sup>The NNMi Causal Engine analyzes the health of your network and provides the ongoing health status reading for each device. The Causal Engine also extensively evaluates problems and determines the root cause for you, whenever possible, sending incidents to notify you of problems. Any incident generated from a Causal Engine management event has an Origin of NNMi in your incident views.

**Outstanding Status Conclusion Values, continued**

Attribute	Description																			
	<table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>CardDown</td> <td>The Operational State of the selected card is Down.</td> <td>Critical</td> <td>Y</td> </tr> </tbody> </table>				Conclusion	Description	Status	Incident?	CardDown	The Operational State of the selected card is Down.	Critical	Y								
Conclusion	Description	Status	Incident?																	
CardDown	The Operational State of the selected card is Down.	Critical	Y																	
	<b>Minor Status Conclusions</b>																			
	<table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>CardDisabled</td> <td>SNMP agent reports that the Administrative State for the selected card is Down.</td> <td>Minor</td> <td>Y</td> </tr> <tr> <td>CardUndeterminedState</td> <td>           NNMI cannot determine the Card's State for one of the following reasons:           <ul style="list-style-type: none"> <li>The SNMP agent responded with a value for the card's Operational Status of Unavailable.</li> <li>The SNMP agent returned a value outside the range of possible values or returned a null value.</li> </ul> </td> <td>Minor</td> <td>Y</td> </tr> <tr> <td>DaughterCardsDown</td> <td>The Operational State of at least one of the associated daughter cards is Down.</td> <td>Minor</td> <td>N</td> </tr> </tbody> </table>				Conclusion	Description	Status	Incident?	CardDisabled	SNMP agent reports that the Administrative State for the selected card is Down.	Minor	Y	CardUndeterminedState	NNMI cannot determine the Card's State for one of the following reasons: <ul style="list-style-type: none"> <li>The SNMP agent responded with a value for the card's Operational Status of Unavailable.</li> <li>The SNMP agent returned a value outside the range of possible values or returned a null value.</li> </ul>	Minor	Y	DaughterCardsDown	The Operational State of at least one of the associated daughter cards is Down.	Minor	N
Conclusion	Description	Status	Incident?																	
CardDisabled	SNMP agent reports that the Administrative State for the selected card is Down.	Minor	Y																	
CardUndeterminedState	NNMI cannot determine the Card's State for one of the following reasons: <ul style="list-style-type: none"> <li>The SNMP agent responded with a value for the card's Operational Status of Unavailable.</li> <li>The SNMP agent returned a value outside the range of possible values or returned a null value.</li> </ul>	Minor	Y																	
DaughterCardsDown	The Operational State of at least one of the associated daughter cards is Down.	Minor	N																	
	<b>Normal Status Conclusions</b>																			
	<table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>CardEnabled</td> <td>The SNMP agent has determined the card's Administrative State is Up.</td> <td>Normal</td> <td>N</td> </tr> <tr> <td>CardUp</td> <td>The Operational State for the current card is Up.</td> <td>Normal</td> <td>N</td> </tr> <tr> <td>DaughterCardsUp</td> <td>The Operational State of all associated daughter cards is Up.</td> <td>Normal</td> <td>N</td> </tr> </tbody> </table>				Conclusion	Description	Status	Incident?	CardEnabled	The SNMP agent has determined the card's Administrative State is Up.	Normal	N	CardUp	The Operational State for the current card is Up.	Normal	N	DaughterCardsUp	The Operational State of all associated daughter cards is Up.	Normal	N
Conclusion	Description	Status	Incident?																	
CardEnabled	The SNMP agent has determined the card's Administrative State is Up.	Normal	N																	
CardUp	The Operational State for the current card is Up.	Normal	N																	
DaughterCardsUp	The Operational State of all associated daughter cards is Up.	Normal	N																	

## Card Form: RegistrationTab

The "Card Form" on page 157 provides details about the selected card.

**For information about each tab:**

### Registration Attributes

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

### Object Identifiers Attributes







Attribute	Description
ID	The Unique Object Identifier, which is unique within the NNMi database.
UUID	The Universally Unique Object Identifier, which is unique across all databases.

## 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 <i>&lt;Card-number / Port-number&gt;</i> .
Hosted on Node	The current value from the Name attribute on the Node form of the 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  Show Analysis or  Open to display more information about the node.
Card	The current value from the Name attribute on the Card form of the card to which this port is assigned.  Click the  Lookup icon and select  Show Analysis or  Open to display more information about the node.
Type	The port-type designator determined by the vendor.
Speed	Potential maximum physical speed of the port.
Configured Duplex Setting	Set by the administrator of the node. Possible values are:

### Basic Attributes, continued

Attribute	Description												
	<p><b>Basic Attributes</b></p> <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Auto</td> <td>Indicates that Auto-negotiation is set for the configured duplex setting. Auto-negotiation is an Ethernet procedure in which two connected devices choose the fastest transmission mode they both support.</td> </tr> <tr> <td>Half</td> <td>Indicates the port supports half-duplex operations. This means the port can send information in both directions between two devices, but in only one direction at a time.</td> </tr> <tr> <td>Full</td> <td>Indicates the port supports full-duplex operations. This means the port can send data in both directions simultaneously.</td> </tr> <tr> <td>Disagree</td> <td>Indicates the port could not agree on the duplex settings with a port on the other end of a connection.</td> </tr> <tr> <td>Unknown</td> <td>Indicates the manufacturer of this device does not support this setting.</td> </tr> </tbody> </table>	Value	Description	Auto	Indicates that Auto-negotiation is set for the configured duplex setting. Auto-negotiation is an Ethernet procedure in which two connected devices choose the fastest transmission mode they both support.	Half	Indicates the port supports half-duplex operations. This means the port can send information in both directions between two devices, but in only one direction at a time.	Full	Indicates the port supports full-duplex operations. This means the port can send data in both directions simultaneously.	Disagree	Indicates the port could not agree on the duplex settings with a port on the other end of a connection.	Unknown	Indicates the manufacturer of this device does not support this setting.
Value	Description												
Auto	Indicates that Auto-negotiation is set for the configured duplex setting. Auto-negotiation is an Ethernet procedure in which two connected devices choose the fastest transmission mode they both support.												
Half	Indicates the port supports half-duplex operations. This means the port can send information in both directions between two devices, but in only one direction at a time.												
Full	Indicates the port supports full-duplex operations. This means the port can send data in both directions simultaneously.												
Disagree	Indicates the port could not agree on the duplex settings with a port on the other end of a connection.												
Unknown	Indicates the manufacturer of this device does not support this setting.												
Associated Interface	<p>The current value from the Name attribute on the Interface form of the interface using this port. This is the current value in NNMI's database obtained using the Interface MIB: ifName, ifAlias, or ifType+ifIndex</p> <p>Click the  Lookup icon and select  Show Analysis or  Open to display more information about the interface.</p>												
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.												
Port Index	The unique value assigned to this port within the card.												

**Related Topics:**

"Node Form" on page 50

"Interface Form" on page 90

"Card Form" on page 157

## Port Form: VLANs Tab

The "Port Form" on the previous page provides details about the selected port.

**For information about each tab:**

(*NNMi Advanced - Global Network Management feature*) There might be slight differences between the VLAN information shown on Regional Managers and Global Managers, because the VLAN calculations use [Layer 2 Connections](#) data.

### 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.  Double-click the row representing a VLAN. The "VLAN Form" on page 156 displays all details about the selected VLAN.

#### Related Topics:

"Node Form" on page 50

"VLAN Form" on page 156

## Port Form: Registration Tab

The "Port Form" on page 171 provides details about the selected port.

#### For information about each tab:

#### Registration Attributes

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

#### Object Identifiers Attributes

Attribute	Description
ID	The Unique Object Identifier, which is unique within the NNMi database.
UUID	The Universally Unique Object Identifier, which is unique across all databases.









## Node Component Form

This form describes the fault and performance metrics used to monitor Node Components. NNMi obtains fault metrics from the node's MIB files.





**Note:** The NNMi administrator can set Node Component thresholds. For more information, see "[Node Form: Node Components Tab](#)" on page 69.

#### 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"</a> on page 179 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"</a> on page 285 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 that has the health attribute 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, HP Network Node Manager iSPI Performance for Metrics Software 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 Node Component table: Small 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>

### Basic Attributes, continued

Attribute	Description
Type	<p>Identifies the aspect of node health that is being monitored. Examples of 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 examples require an HP Network Node Manager iSPI Performance for Metrics Software 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>
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> <p> <b>Managed</b> – Indicates the node is managed by NNMi.</p> <p> <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.</p> <p> <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.</p> <p>This attribute is useful for notifying NNMi when a device has been temporarily out of service, or should never be managed.</p> <p><b>Note:</b> If the Security configuration permits, you can change this setting using <b>Actions</b> → <b>Management Mode</b>.</p> <p><b>Tip:</b> You can right-click any object in a table or map view to access the <b>Actions</b> menu.</p>
Direct Management Mode	<p>Indicates whether the current node component is being managed. This attribute is set by the administrator and specifies whether a node component should be managed or whether a node component is temporarily out of service. Possible values are:</p> <p> <b>Inherited</b> – Used to indicate that the node component should inherit the Management Mode from the node in which it resides.</p>

### Basic Attributes, continued

Attribute	Description
	<p> <b>Not Managed</b> – Used to indicate that NNMi does not discover or monitor the node component.</p> <p> <b>Out of Service</b> – Used to indicate a node component is unavailable because it is out of service. NNMi does not discover or monitor these node components.</p> <p>This attribute is useful for notifying NNMi when a node component, such as a fan, is temporarily out of service, or should never be managed.</p> <p><b>Note:</b> If you change the Direct Management Mode using <b>Actions</b> → <b>Management Mode</b>, 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	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).

## Node Component Form: Monitored Attributes Tab

The "Node Component Form" on page 173 provides details about the monitored attributes related to the current node component. The State of monitored attributes can be influenced by thresholds configured by your NNMi administrator.

For information about each tab:

### Attributes Table

Description
<p>Table view of the Name and <a href="#">State</a> of each monitored attribute associated with the selected Node Component. Use this view to determine the State of each monitored attribute.</p> <p>Double-click the row representing a Monitored Attribute. The "Node Component Monitored Attribute Form" below displays all details about the selected Monitored Attribute.</p>

## Node Component Monitored Attribute Form

The Monitored Attribute form displays information about the attribute selected on the Attribute tab of the "Node Component Form" on page 173.

Fault metrics are available for the following Node Components:

- Fan
- Management Address ICMP Response Time



- Power Supply
- Temperature
- Voltage

NNMi obtains fault metric information from the associated MIB.














*(NNM iSPI Performance for Metrics)* If the HP Network Node Manager iSPI Performance for Metrics Software software is installed and configured within your environment, the NodeComponent: Monitored Attributes 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:

- Backplane Utilization
- Buffer Failure Rate
- Buffer Miss Rate
- Buffer Utilization
- CPU 5Sec Utilization
- CPU 1Min Utilization
- CPU 5Min Utilization
- Disk Space Utilization
- Memory Utilization




**Basics Attributes**

Attribute	Description
Name	<p>Name used to identify the attribute being monitored.</p> <p>The number of attributes available vary depending on the number of MIBs available for the current node component. See "<a href="#">Node Component Form</a>" on page 173 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>
Unique Key	Used as a unique identifier for the Node Health Monitored Attribute. Any Node Health Monitored Attribute provided by NNMi begins with the prefix <code>com.hp.nms.</code>
State	Normalized value used to indicate the State of the attribute of the selected node.

## Basics Attributes, continued

Attribute	Description
	<p>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 might 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> <p>The following values indicate NNMi could not gather the required data:</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 this agent.</li><li> <b>No Polling Policy</b> - Indicates the object is being polled, but no polling policy exists in Monitoring Configuration settings for this monitored attribute.</li><li> <b>Not Polled</b> - Indicates that this 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. This object attribute might or might not have an associated polling policy.</li><li> <b>Unavailable</b> - Unable to determine the State. For example, the SNMP agent returned a value outside the range of possible values or returned a null value.</li><li> <b>Unset</b> – Currently not used by NNMi.</li></ul> <p><b>Note:</b> State is determined by the State Poller Service. Only the Fan and Power Supply Node Components' States contribute towards the status calculation for the node. See the <a href="#">Status tab</a> for more information.</p> <p>(NNM iSPI Performance for Metrics) Additional States for performance metrics include the following (<b>Warning</b> and <b>Critical</b> states are not used for performance metrics):</p> <ul style="list-style-type: none"><li> <b>Abnormal Range</b> – Indicates State Poller has collected values outside the normal range when compared to the baseline data collected for the current object.</li><li> <b>Normal</b> - Indicates there are no known problems related to the associated object.</li><li> <b>Normal Range</b> - Indicates State Poller collected values within the normal range when compared to the baseline data collected for the current object.</li></ul>

### Basics Attributes, continued

Attribute	Description
	 <b>High</b> - The High threshold was crossed.  <b>Low</b> - The Low threshold was crossed.  <b>None</b> - The threshold value returned is zero.
Last Modified	The most recent date and time when the State of this Monitored Attribute changed.

## Node Component Form: Incidents Tab

**Tip:** See "Incident Form" on page 311 for more details about the incident attributes that appear in the incident view's column headings.

The "Node Component Form" on page 173 provides details about the monitored attributes for the selected node.

**For information about each tab:**

### Incidents Table





Description
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.  Double-click the row representing an incident. The "Incident Form" on page 311 displays all details about the selected incident.

## Node Component Form: Status Tab





The "Node Component Form" on page 173 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. Possible values are:  No Status  Normal  Disabled  Unknown

### Overall Status, continued

Attribute	Description
	 Warning  Minor  Major  Critical  <p><b>Note:</b> Your NNMi administrator might have disabled polling of Node Component 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</a>" below. Status reflects the most serious outstanding conclusion. See "<a href="#">Watch Status Colors</a>" on page 285 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 Table

Attribute	Description
Status History	<p>List of the last 30 changes in the status for the node component. This view is useful for obtaining a summary of the node component status so that you can better determine any patterns in behavior and activity.</p> <p>Double-click the row representing a Status History. The Status History form displays all details about the selected Status.</p>

## Node Component Form: Conclusions Tab

The "[Node Component Form](#)" on page 173 provides details about the selected health metric for the current node.

**For information about each tab:**

### Outstanding Status Conclusion Values

Attribute	Description
Outstanding Status Conclusion	The dynamically generated list of summary statuses of the monitored attribute that contributed to the current overall status of the selected node. Status is set by the Causal Engine.

**Outstanding Status Conclusion Values, continued**

Attribute	Description												
s	<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 component's most current Status.</p> <p>The status value is correlated based on the most critical conclusions.</p> <p>Double-click the row representing a Status Conclusion. The Status Conclusion form displays all details about the selected Status Conclusion.</p> <p>The following table describes the possible Conclusions that might appear for a node object.</p> <p><b>Note:</b> A Y in the <b>Incident?</b> column indicates that the Conclusion results in an incident.</p> <p><b>Critical Status Conclusions</b></p> <table border="1" data-bbox="451 856 1377 1848"> <thead> <tr> <th data-bbox="451 863 966 947">Conclusion</th> <th data-bbox="971 863 1133 947">Description</th> <th data-bbox="1138 863 1239 947">Status</th> <th data-bbox="1243 863 1377 947">Incident?</th> </tr> </thead> <tbody> <tr> <td data-bbox="451 953 966 1346">BackplaneOutOfRangeOrMalfunctioning</td> <td data-bbox="971 953 1133 1346">The backplane monitored attributes are outside of the threshold range configured for the device.</td> <td data-bbox="1138 953 1239 1346">Critical</td> <td data-bbox="1243 953 1377 1346">Y</td> </tr> <tr> <td data-bbox="451 1352 966 1841">BufferOutOfRangeOrMalfunctioning</td> <td data-bbox="971 1352 1133 1841">The buffer pool monitored attributes are outside of the threshold range configured for the device. This incident indicates the buffer</td> <td data-bbox="1138 1352 1239 1841">Critical</td> <td data-bbox="1243 1352 1377 1841">Y</td> </tr> </tbody> </table>	Conclusion	Description	Status	Incident?	BackplaneOutOfRangeOrMalfunctioning	The backplane monitored attributes are outside of the threshold range configured for the device.	Critical	Y	BufferOutOfRangeOrMalfunctioning	The buffer pool monitored attributes are outside of the threshold range configured for the device. This incident indicates the buffer	Critical	Y
Conclusion	Description	Status	Incident?										
BackplaneOutOfRangeOrMalfunctioning	The backplane monitored attributes are outside of the threshold range configured for the device.	Critical	Y										
BufferOutOfRangeOrMalfunctioning	The buffer pool monitored attributes are outside of the threshold range configured for the device. This incident indicates the buffer	Critical	Y										

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		pool is exhausted or cannot meet the demand.		
	CpuOutOfRangeOrMalfunctioning	Any of the following utilization averages is above the threshold range configured for the device: <ul style="list-style-type: none"> <li>• CPU 5 second utilization</li> <li>• CPU 1 minute utilization</li> <li>• CPU 5 minute utilization</li> </ul>	Critical	Y
	DiskOutOfRangeOrMalfunctioning	The disk monitored attributes are outside of the threshold range configured for the device.	Critical	Y
	FanOutOfRangeOrMalfunctioning	The fan monitored	Critical	Y

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		attributes are outside of the threshold range configured for the device.		
	MemoryOutOfRangeOrMalfunctioning	The Source Node's memory pool is outside of the threshold range configured for the device.  This incident indicates the memory pool is exhausted or cannot meet the demand for use.	Critical	Y
	PowerSupplyOutOfRangeOrMalfunctioning	A power supply's monitored attributes are outside of the threshold range configured for the device.	Critical	Y

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
	TemperatureOutOfRangeOrMalfunctioning	The specified temperature sensor on the Source Node is outside of the threshold range configured for the device.	Critical	Y
	VoltageOutOfRangeOrMalfunctioning	The specified voltage on one of the Source Node's power supplies is outside of the threshold configured for the device.	Critical	Y
	<b>Warning Status Conclusions</b>			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
	BackplaneAbnormal	The backplane utilization is abnormal based on the computed baseline.	Warning	Y
	BufferAbnormal	The buffer utilization is abnormal based on the computed baseline.	Warning	Y
	CpuAbnormal	The CPU utilization is abnormal based on the computed baseline for one of the following: <ul style="list-style-type: none"> <li>• CPU 5 second utilization</li> </ul>	Warning	Y



**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
		<ul style="list-style-type: none"> <li>CPU 1 minute utilization</li> <li>CPU 5 minute utilization</li> </ul>		
	DiskAbnormal	The disk space utilization is abnormal based on the computed baseline.	Warning	Y
	MemoryAbnormal	The memory utilization is abnormal based on the computed baseline.	Warning	Y
	<b>Normal Status Conclusions</b>			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
	BackplaneInRangeAndFunctioning	The backplane monitored attributes are within the threshold range configured for the device.	Normal	N
	BackplaneNormal	The backplane utilization is normal based on the computed baseline.	Normal	N
	BufferInRangeAndFunctioning	The buffer pool is operating within the threshold range configured for the device.	Normal	N
	BufferNormal	The buffer utilization is normal based on the computed baseline.	Normal	N
	CpuInRangeAndFunctioning	All of the following utilization averages are within the	Normal	N

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		threshold range configured for the device: <ul style="list-style-type: none"> <li>• CPU 5 second utilization</li> <li>• CPU 1 minute utilization</li> <li>• CPU 5 minute utilization</li> </ul>		
	CpuNormal	The CPU utilization is normal based on the computed baseline for the following: <ul style="list-style-type: none"> <li>• CPU 5 second utilization</li> <li>• CPU 1 minute utilization</li> <li>• CPU 5 minute utilization</li> </ul>	Normal	N
	DiskInRangeAndFunctioning	The disk monitored attributes are within the threshold range configured for the device.	Normal	N
	DiskNormal	The disk space utilization is normal based on the computed baseline.	Normal	N
	FanInRangeAndFunctioning	The specified fan monitored attributes are	Normal	N

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	Conclusion	Description	Status	Incident?
		within the threshold range configured for the device.		
	MemoryInRangeAndFunctioning	The specified memory pool is operating within the threshold range configured for the device.	Normal	N
	MemoryNormal	The memory utilization is normal based on the computed baseline.	Normal	N
	PowerSupplyInRangeAndFunctioning	A power supply's monitored attributes are within the threshold range configured for the device.	Normal	N
	TemperatureInRangeAndFunctioning	The specified temperature sensor on the Source Node is within the threshold range configured for the device.	Normal	N
	VoltageInRangeAndFunctioning	The specified voltage on one of the Source Node's power supplies is within the threshold range configured for the device.	Normal	N

## Node Component Form: Registration Tab

The "Node Component Form" on page 173 provides details about the selected Node Component.

For information about each tab:

### Registration Attributes

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

### Object Identifiers Attributes

Attribute	Description
ID	The Unique Object Identifier, which is unique within the NNMi database.
UUID	The Universally Unique Object Identifier, which is unique across all databases.

## 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. The NNMi administrator can configure NNMi to automatically delete Layer 2 Connections when all member Interfaces are down for a specified number of days.

For information about each tab:










**Note:** Forwarding Database (FDB) information can cause NNMi to establish wrong Layer 2 Connections in the following cases:

- When the FDB is configured as cache and contains obsolete data.
- In network environments with hardware from a variety of vendors, when each vendor generates different and sometimes conflicting FDB data.

*Optional:* NNMi administrators can configure Spiral Discovery to ignore the FDB data from one Node Group when calculating Layer 2 Connections (the FDB data is still included in other calculations).


*(NNMi Advanced - Global Network Management feature)* NNMi must read the Forwarding Database (FDB) tables from Ethernet switches within the network before accurate communication paths between these network devices can be calculated. Because the FDB data is involved, NNMi can produce different results on a Regional Manager as opposed to the Global Manager.

### 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	<p>Overall status for the current connection. NNMi follows the ISO standard for status classification. See the "<a href="#">Layer 2 Connection Form: Status Tab</a>" on page 192 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="#">Layer 2 Connection Form: Conclusions Tab</a>" on page 193. Status reflects the most serious outstanding conclusion. See "<a href="#">Watch Status Colors</a>" on page 285 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>Note:</b> (NNMi Advanced) Layer 2 Connections using <a href="#">Link Aggregation</a><sup>1</sup> protocols can connect sets of Interfaces. See "<a href="#">Layer 2 Connection Form: Link Aggregation Tab (NNMi Advanced)</a>" on page 199. These Aggregator Layer 2 Connections display as thick lines on NNMi maps.</p> <p>If you see the  icon, NNMi gathered information from Layer 2 of the Open System Interconnection (OSI) networking model to detect this connection. Layer 2 is the Data Link layer that encodes and decodes data packets into bits. The Data Link layer has two sub-layers: The Media Access Control (MAC) sub-layer controls how a computer gains access to data and permission to transmit the data. The Logical Link Control</p>

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

**Basic Attributes, continued**

Attribute	Description
	<p>(LLC) sub-layer controls frame synchronization, flow control, and error checking. The following are some examples of possible Topology Source values:</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 switch)</p> <p><b>FDBH</b> - NNMi's Forwarding Database High Priority indicates a special case was encountered and NNMi gave priority of FDB over Discovery Protocol information.</p> <p><b>FDP</b> - Foundry Discovery Protocol</p> <p><b>LLDP</b> - Link Layer Discovery Protocol</p> <p><b>NDP</b> - IPv6 Neighbor Discovery Protocol</p> <p><b>SONMP</b> - SynOptics Network Management Protocol</p> <p><b>ROUTES</b> - indicates NNMi creates the connection from the routing data. NNMi creates these Layer 2 Connections for <i>unnumbered</i> interfaces. For more information, see the "NNMi Discovery" chapter of the <i>HP Network Node Manager i Software Deployment Reference</i>, which is available at:  <a href="http://h20230.www2.hp.com/selfsolve/manuals">http://h20230.www2.hp.com/selfsolve/manuals</a>.</p> <p><b>SUBNETCONNECTION</b>- Subnet Connection Rule. NNMi applied a special configurable rule for subnets (only those IPv4 subnets with a prefix length between 28 and 31) to detect this connection. NNMi gathers information from Layer 3 of the Open System Interconnection (OSI) networking model to detect this connection. Layer 3 is the Network layer that provides switching, routing, and logical paths (virtual circuits) for transmitting data between nodes. The NNMi administrator configures the Subnet Connection Rules, see "Help for Administrators" for more information. On the NNMi map, the following icon is in the middle of the SUBNETCONNECTION line:</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>(<i>NNMi Advanced - Global Network Management feature</i>) The text you enter here is not sent from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager can add notes that are stored in the NNMi database on the Global Manager.</p> <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>

### Basic Attributes, continued

Attribute	Description
	Type a maximum of 1024 characters. Alpha-numeric, spaces, and special characters (~ ! @ # \$ % ^ & * ( ) _ + -) are permitted.

## Layer 2 Connection Form: Interfaces Tab

The "Layer 2 Connection Form" on page 188 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>Double-click the row representing an interface. The "Interface Form" on page 90 displays all details about the selected interface.</p>

## Layer 2 Connection Form: Incidents Tab

The "Layer 2 Connection Form" on page 188 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. NNMI displays only those incidents that have a Family attribute value of <code>Connection</code>.</p> <p><b>Tip:</b> To check all Incidents related to the Interface on each end of the connection, navigate to the "Layer 2 Connection Form: Interfaces Tab" above and open an Interface form. To check all incidents related to the Node, use the <b>Hosted On Node</b> attribute on the Interface form to open the Node form.</p> <p>Examples of the incidents that might appear as Associated Incidents for Layer 2 Connections include the following:</p> <ul style="list-style-type: none"><li>• "Connection Down" on page 397</li><li>• Modified Connection Down</li></ul> <p>Associated 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>

### Incidents Table, continued









Attribute	Description
	Double-click the row representing an incident. The "Incident Form" on page 311 displays all details about the selected incident. Navigate to the "Incident Form: Correlated Children Tab" on page 320 and "Incident Form: Correlated Parents Tab" on page 320 to check for any correlated incidents that are associated with the interfaces and nodes on each end of the connection.

## Layer 2 Connection Form: Status Tab

The "Layer 2 Connection Form" on page 188 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> <p><b>Note:</b> The icons are displayed only in table views.</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 "Layer 2 Connection Form: Conclusions Tab" on the next page. Status reflects the most serious outstanding conclusion. See "Watch Status Colors" on page 285 for more information about possible status values.</p>



### Status Attributes, continued

Attribute	Description
	<i>NNMi Advanced</i> . <a href="#">Link Aggregation</a> <sup>1</sup> : If the Layer 2 Connection is an Aggregator, the Status is calculated using the combined Status of all Aggregation Member Layer 2 Connections. For more information, see " <a href="#">Layer 2 Connection Form: Link Aggregation Tab (NNMi Advanced)</a> " on page 199 and <a href="#">Status Color for Aggregator Objects</a> .
Status Last Modified	Date and time indicating when the status was last set.

### Status History Table

Attribute	Description
Status History	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.  Double-click the row representing a Status History. The Status History form displays all details about the selected Status.

## Layer 2 Connection Form: Conclusions Tab

The "[Layer 2 Connection Form](#)" on page 188 provides details about a managed connection.

All relevant conclusions are shown in the table on this tab. The most severe Status in the current group of conclusions becomes the overall L2 Connection status. Some L2 Connection conclusions propagate to other object types:

**For information about each tab:**

### Outstanding Status Conclusion Values

Attribute	Description
Outstanding Status Conclusions	The dynamically generated list of summary statuses of the connection that contributed to the current overall Status of the selected connection. Status is set by Causal Engine.  Each Conclusion listed is still outstanding and applies to the current overall Status.

---

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

### Outstanding Status Conclusion Values, continued

Attribute	Description												
	<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>The Status value is correlated based on the most critical Conclusion.</p> <p>Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion.</p> <p>The following table describes the possible Conclusions that might appear for a Connection object.</p> <p><b>Note:</b> A <b>Y</b> in the <b>Incident?</b> column indicates that the Conclusion results in an incident.</p> <p><b>Critical Status Conclusions</b></p> <table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>AggregatorLinkDown</td> <td>(NNMi Advanced) <a href="#">Link Aggregation</a><sup>1</sup>: The Operational State of <i>all</i> participating Aggregation Member Layer 2 Connections is Down. For more information, see "Layer 2 Connection Form: Link Aggregation Tab (NNMi Advanced)" on page 199.</td> <td>Critical</td> <td>Y</td> </tr> <tr> <td>AllConnectionThresholdValuesHigh</td> <td>Each interface in the connection contains one of the following Conclusions:           <ul style="list-style-type: none"> <li>• InterfacelInputUtilizationHigh</li> <li>• InterfaceOutputUtilizationHigh</li> <li>• InterfacelInputDiscardRateHigh</li> </ul> </td> <td>Critical</td> <td>N</td> </tr> </tbody> </table>	Conclusion	Description	Status	Incident?	AggregatorLinkDown	(NNMi Advanced) <a href="#">Link Aggregation</a> <sup>1</sup> : The Operational State of <i>all</i> participating Aggregation Member Layer 2 Connections is Down. For more information, see "Layer 2 Connection Form: Link Aggregation Tab (NNMi Advanced)" on page 199.	Critical	Y	AllConnectionThresholdValuesHigh	Each interface in the connection contains one of the following Conclusions: <ul style="list-style-type: none"> <li>• InterfacelInputUtilizationHigh</li> <li>• InterfaceOutputUtilizationHigh</li> <li>• InterfacelInputDiscardRateHigh</li> </ul>	Critical	N
Conclusion	Description	Status	Incident?										
AggregatorLinkDown	(NNMi Advanced) <a href="#">Link Aggregation</a> <sup>1</sup> : The Operational State of <i>all</i> participating Aggregation Member Layer 2 Connections is Down. For more information, see "Layer 2 Connection Form: Link Aggregation Tab (NNMi Advanced)" on page 199.	Critical	Y										
AllConnectionThresholdValuesHigh	Each interface in the connection contains one of the following Conclusions: <ul style="list-style-type: none"> <li>• InterfacelInputUtilizationHigh</li> <li>• InterfaceOutputUtilizationHigh</li> <li>• InterfacelInputDiscardRateHigh</li> </ul>	Critical	N										

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

### Outstanding Status Conclusion Values, continued

Attribute		Description													
	<table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td></td> <td> <ul style="list-style-type: none"> <li>InterfaceOutputDiscardRateHigh</li> <li>InterfaceInputErrorRateHigh</li> <li>InterfaceOutputErrorRateHigh</li> <li>InterfaceOutputQueueDropsRateHigh</li> <li>InterfaceInputQueueDropsRateHigh</li> <li>InterfaceFCSWLANErrorRateHigh</li> <li>InterfaceFCSLANErrorRateHigh</li> </ul> </td> <td></td> <td></td> </tr> <tr> <td>ConnectionDown</td> <td>Both (or all) ends of a connection have an Operational State of Down.</td> <td>Critical</td> <td>Y</td> </tr> </tbody> </table>	Conclusion	Description	Status	Incident?		<ul style="list-style-type: none"> <li>InterfaceOutputDiscardRateHigh</li> <li>InterfaceInputErrorRateHigh</li> <li>InterfaceOutputErrorRateHigh</li> <li>InterfaceOutputQueueDropsRateHigh</li> <li>InterfaceInputQueueDropsRateHigh</li> <li>InterfaceFCSWLANErrorRateHigh</li> <li>InterfaceFCSLANErrorRateHigh</li> </ul>			ConnectionDown	Both (or all) ends of a connection have an Operational State of Down.	Critical	Y		
Conclusion	Description	Status	Incident?												
	<ul style="list-style-type: none"> <li>InterfaceOutputDiscardRateHigh</li> <li>InterfaceInputErrorRateHigh</li> <li>InterfaceOutputErrorRateHigh</li> <li>InterfaceOutputQueueDropsRateHigh</li> <li>InterfaceInputQueueDropsRateHigh</li> <li>InterfaceFCSWLANErrorRateHigh</li> <li>InterfaceFCSLANErrorRateHigh</li> </ul>														
ConnectionDown	Both (or all) ends of a connection have an Operational State of Down.	Critical	Y												
<b>Minor Status Conclusions</b>															
	<table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>AggregatorLinkDegraded</td> <td>(NNMi Advanced) <a href="#">Link Aggregation</a><sup>1</sup>: Some (but not all) of the participating Aggregation Member Layer 2 Connections have an Operational State of Down. For more information, see "<a href="#">Layer 2 Connection Form: Link Aggregation Tab (NNMi</a></td> <td>Minor</td> <td>Y</td> </tr> </tbody> </table>	Conclusion	Description	Status	Incident?	AggregatorLinkDegraded	(NNMi Advanced) <a href="#">Link Aggregation</a> <sup>1</sup> : Some (but not all) of the participating Aggregation Member Layer 2 Connections have an Operational State of Down. For more information, see " <a href="#">Layer 2 Connection Form: Link Aggregation Tab (NNMi</a>	Minor	Y						
Conclusion	Description	Status	Incident?												
AggregatorLinkDegraded	(NNMi Advanced) <a href="#">Link Aggregation</a> <sup>1</sup> : Some (but not all) of the participating Aggregation Member Layer 2 Connections have an Operational State of Down. For more information, see " <a href="#">Layer 2 Connection Form: Link Aggregation Tab (NNMi</a>	Minor	Y												

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

**Outstanding Status Conclusion Values, continued**

Attribute		Description		Stat	Incide
		Conclusion	Description	us	nt?
			Advanced)" on page 199.		
	ConnectionWithAtLeastOneDownEP		At least one interface, but not all interfaces, in the connection have an Operational State of Down.	Minor	N
	SomeConnectionThresholdValuesHigh		<p>One interface in the connection contains one of the following conclusions:</p> <ul style="list-style-type: none"> <li>• InterfaceInputUtilizationHigh</li> <li>• InterfaceOutputUtilizationHigh</li> <li>• InterfaceInputDiscardRateHigh</li> <li>• InterfaceOutputDiscardRateHigh</li> <li>• InterfaceInputErrorRateHigh</li> <li>• InterfaceOutputErrorRateHigh</li> <li>• InterfaceOutputQueueDropRateHigh</li> <li>• InterfaceInputQueueDropRateHigh</li> <li>• InterfaceFCSWLANErrorRateHigh</li> <li>• InterfaceFCSLANErrorRateHigh</li> </ul>	Minor	N

**Outstanding Status Conclusion Values, continued**

Attribute		Description	
Conclusion	Description	Status	Incident?
	eHigh		
SomeOrAllConnectionThresholdValuesLow	One interface in the connection contains one of the following conclusions: <ul style="list-style-type: none"> <li>• InterfaceInputUtilizationLow</li> <li>• InterfaceOutputUtilizationLow</li> </ul>	Minor	N
SomeOrAllConnectionThresholdValuesNone	One interface in the connection contains one of the following conclusions: <ul style="list-style-type: none"> <li>• InterfaceInputUtilizationNone</li> <li>• InterfaceOutputUtilizationNone</li> <li>• InterfaceInputDiscardRateNone</li> <li>• InterfaceOutputDiscardRateNone</li> <li>• InterfaceInputErrorRateNone</li> <li>• InterfaceOutputErrorRateNone</li> </ul>	Minor	N
<b>Warning Status Conclusions</b>			
Conclusion	Description	Status	Incident?
ConnectionPartiallyUnresponsive	At least one interface in a connection has an Operational State of Up and at least one interface's associated SNMP Agent is not responding to	Warning	N

### Outstanding Status Conclusion Values, continued

Attribute		Description			
		<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
			SNMP queries.		
<b>Unknown Status Conclusions</b>					
		<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
		ConnectionUnknown	All SNMP Agents associated with all interfaces in the connection are not responding to SNMP queries.	Unknown	N
<b>Disabled Status Conclusions</b>					
		<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
		ConnectionDisabled	All interfaces in the connection have an Administrative State of Disabled.	Disabled	N
		ConnectionWithAtLeastOneDisabledEP	At least one interface, but not all interfaces, in the connection have an Administrative State of Down.	Disabled	N
<b>Normal Status Conclusions</b>					
		<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
		AggregatorLinkUp	(NNMi Advanced) <a href="#">Link Aggregation</a> <sup>1</sup> : All	Normal	N

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

**Outstanding Status Conclusion Values, continued**

Attribute		Description		
Conclusion	Description	Status	Incident?	
	of the participating Aggregation Member Layer 2 Connections have an Operational State of Up. For more information, see "Layer 2 Connection Form: Link Aggregation Tab (NNMi Advanced)" below.			
ConnectionEnabled	All interfaces in a connection have an Administrative State of Up.	Normal	N	
ConnectionUp	The Operational State of each interface in the connection is Up.	Normal	N	
ConnectionWithinThresholdBoundaries	All thresholds on interfaces in the connection are functioning within the threshold boundaries set on the device.	Normal	N	

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

The "Layer 2 Connection Form" on page 188 provides details about the selected Layer 2 Connection.

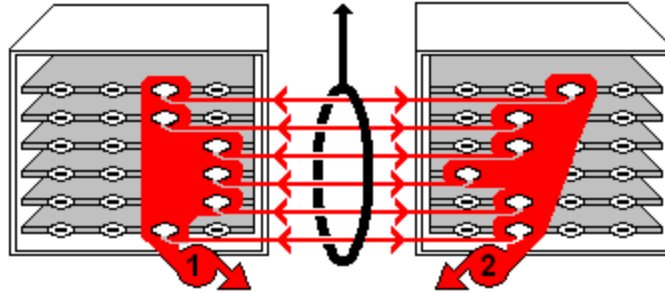
**For information about each tab:**

The Layer 2 Connection Form: Link Aggregation Tab appears if the selected connection uses a [Link Aggregation](#)<sup>1</sup> protocol.

### Example Link Aggregation

Thick Line on Layer 2 Neighbor View Map =  
one Aggregator Layer 2 Connection:

- Logical unit (not physical)
- Functions as if it were one
- 6 Aggregation Member Layer 2 Connections



two Aggregator Interfaces:

- Logical units (not physical)
- Each functions as if it were one
- Each has 6 Aggregation Member Interfaces

The selected object's *role* in the Link Aggregation determines the contents of the tab:

---



<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.



- **Aggregation Member**, click here for details.

Attribute	Description																
Link Aggregation Protocol	<p>The <b>Link Aggregation</b><sup>1</sup> Protocol currently in use. These protocols allow network administrators to configure a <i>set of interfaces</i> on a switch as one <i>Aggregator Interface</i>, creating an Aggregator Layer 2 Connection to another device using multiple interfaces in parallel to increase bandwidth, increase the speed at which data travels, and increase redundancy:</p> <table border="1"> <thead> <tr> <th>Text</th> <th>Represents This Protocol</th> </tr> </thead> <tbody> <tr> <td>Cisco Port Aggregation Protocol</td> <td>Cisco Systems Port Aggregation Protocol (pagp)</td> </tr> <tr> <td>Nortel Multi-Link Trunking</td> <td>Nortel Multi-Link Trunk technology (mlt)</td> </tr> <tr> <td>Split MLT</td> <td>Split Multi-Link Trunk: configuration technology (splitMlt)</td> </tr> <tr> <td>Inter-Switch Trunk MLT</td> <td>Split Multi-Link Trunk: inter-switch trunk (istMlt)</td> </tr> <tr> <td>802.3ad Link Aggregation Control Protocol</td> <td>IEEE 802.3ad Link Aggregation Control protocol (LACP)</td> </tr> <tr> <td>Static/Manual Configured Link Aggregation</td> <td>Static/Manual Configured Link Aggregation</td> </tr> <tr> <td>Unknown Protocol Link Aggregation</td> <td>unknown</td> </tr> </tbody> </table> <p><b>Note:</b> It is possible for a Layer 2 Connection to connect sets of Aggregator/Member Interfaces that are configured using different Link Aggregation protocols. In that case, this attribute value contains multiple protocols separated with a slash (/).</p>	Text	Represents This Protocol	Cisco Port Aggregation Protocol	Cisco Systems Port Aggregation Protocol (pagp)	Nortel Multi-Link Trunking	Nortel Multi-Link Trunk technology (mlt)	Split MLT	Split Multi-Link Trunk: configuration technology (splitMlt)	Inter-Switch Trunk MLT	Split Multi-Link Trunk: inter-switch trunk (istMlt)	802.3ad Link Aggregation Control Protocol	IEEE 802.3ad Link Aggregation Control protocol (LACP)	Static/Manual Configured Link Aggregation	Static/Manual Configured Link Aggregation	Unknown Protocol Link Aggregation	unknown
Text	Represents This Protocol																
Cisco Port Aggregation Protocol	Cisco Systems Port Aggregation Protocol (pagp)																
Nortel Multi-Link Trunking	Nortel Multi-Link Trunk technology (mlt)																
Split MLT	Split Multi-Link Trunk: configuration technology (splitMlt)																
Inter-Switch Trunk MLT	Split Multi-Link Trunk: inter-switch trunk (istMlt)																
802.3ad Link Aggregation Control Protocol	IEEE 802.3ad Link Aggregation Control protocol (LACP)																
Static/Manual Configured Link Aggregation	Static/Manual Configured Link Aggregation																
Unknown Protocol Link Aggregation	unknown																
Aggregator	<p>Name of the Aggregator that <i>contains</i> the selected participating Aggregation Member:</p> <ul style="list-style-type: none"> <li>■ Aggregator Interface - represents multiple member interfaces</li> <li>■ Aggregator Layer 2 Connection - thick line on the Layer 2 Neighbor View map represents multiple member Layer 2 Connections</li> </ul>																

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

Attribute	Description
	<p>See <a href="#">Layer 2 Neighbor View Map Objects</a> for more information.</p> <p>Click the  Lookup icon, and choose  Open to open the form for the Aggregator.</p>

- **Aggregator** (representing multiple members), click here for details.

Attribute	Description																
Link Aggregation Protocol	<p>The <b>Link Aggregation</b><sup>1</sup> Protocol currently in use. These protocols allow network administrators to configure a <i>set of interfaces</i> on a switch as one <i>Aggregator Interface</i>, creating an Aggregator Layer 2 Connection to another device using multiple interfaces in parallel to increase bandwidth, increase the speed at which data travels, and increase redundancy:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #003366; color: white;">Text</th> <th style="background-color: #003366; color: white;">Represents This Protocol</th> </tr> </thead> <tbody> <tr> <td>Cisco Port Aggregation Protocol</td> <td>Cisco Systems Port Aggregation Protocol (pagp)</td> </tr> <tr> <td>Nortel Multi-Link Trunking</td> <td>Nortel Multi-Link Trunk technology (mlt)</td> </tr> <tr> <td>Split MLT</td> <td>Split Multi-Link Trunk: configuration technology (splitMlt)</td> </tr> <tr> <td>Inter-Switch Trunk MLT</td> <td>Split Multi-Link Trunk: inter-switch trunk (istMlt)</td> </tr> <tr> <td>802.3ad Link Aggregation Control Protocol</td> <td>IEEE 802.3ad Link Aggregation Control protocol (LACP)</td> </tr> <tr> <td>Static/Manual Configured Link Aggregation</td> <td>Static/Manual Configured Link Aggregation</td> </tr> <tr> <td>Unknown Protocol Link Aggregation</td> <td>unknown</td> </tr> </tbody> </table> <p><b>Note:</b> It is possible for a Layer 2 Connection to connect sets of Aggregator/Member Interfaces that are configured using different Link Aggregation protocols. In that case, this attribute value contains multiple protocols separated with a slash (/).</p>	Text	Represents This Protocol	Cisco Port Aggregation Protocol	Cisco Systems Port Aggregation Protocol (pagp)	Nortel Multi-Link Trunking	Nortel Multi-Link Trunk technology (mlt)	Split MLT	Split Multi-Link Trunk: configuration technology (splitMlt)	Inter-Switch Trunk MLT	Split Multi-Link Trunk: inter-switch trunk (istMlt)	802.3ad Link Aggregation Control Protocol	IEEE 802.3ad Link Aggregation Control protocol (LACP)	Static/Manual Configured Link Aggregation	Static/Manual Configured Link Aggregation	Unknown Protocol Link Aggregation	unknown
Text	Represents This Protocol																
Cisco Port Aggregation Protocol	Cisco Systems Port Aggregation Protocol (pagp)																
Nortel Multi-Link Trunking	Nortel Multi-Link Trunk technology (mlt)																
Split MLT	Split Multi-Link Trunk: configuration technology (splitMlt)																
Inter-Switch Trunk MLT	Split Multi-Link Trunk: inter-switch trunk (istMlt)																
802.3ad Link Aggregation Control Protocol	IEEE 802.3ad Link Aggregation Control protocol (LACP)																
Static/Manual Configured Link Aggregation	Static/Manual Configured Link Aggregation																
Unknown Protocol Link Aggregation	unknown																

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

Attribute	Description
Available Bandwidth	Sum of the interface Input Speed attribute values of the Member Interfaces that have a MIB-II ifOperStatus that 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 Aggregation Members.</p> <p>For more information, double-click the row representing an Aggregation Member:</p> <ul style="list-style-type: none"> <li>▪ The "Interface Form" on page 90 displays all details about the selected Interface.</li> <li>▪ The "Layer 2 Connection Form" on page 188 displays all details about the selected Layer 2 Connection.</li> </ul>

## Layer 2 Connection Form: Registration Tab

The "Layer 2 Connection Form" on page 188 provides details about a managed connection.

**For information about each tab:**

### Registration Attributes

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

### Object Identifiers Attributes

Attribute	Description
ID	The Unique Object Identifier, which is unique within the NNMi database.
UUID	The Universally Unique Object Identifier, which is unique across all databases.









## Card Redundancy Group Form

Card Redundancy Groups are configured to provide one-to-one redundancy protection against processor card failure.

The Card Redundancy Group form provides details about the Card Redundancy Group you selected. The following table describes the fields included on the Card Redundancy Group form.

**For information about each tab:**

### Basic Attributes

Attribute	Description						
Name	<p>Name assigned to the Card Redundancy Group. NNMi uses the Node Name followed by a slash and then the name that is specific to the Device Vendor:</p> <p><b>Card Redundancy Group Naming Conventions</b></p> <table border="1"> <thead> <tr> <th>Device Vendor</th> <th>Naming Convention</th> </tr> </thead> <tbody> <tr> <td>Cisco</td> <td> <p>&lt;nodename&gt;/Supervisor Engine Group</p> <p><b>Note:</b> Only cards classified as Management Modules are considered for Card Redundancy Groups.</p> </td> </tr> <tr> <td>HP ProCurve</td> <td> <p>&lt;nodename&gt;/Management Module Group</p> <p><b>Note:</b> Only cards classified as Management Modules are considered for Card Redundancy Groups.</p> </td> </tr> </tbody> </table>	Device Vendor	Naming Convention	Cisco	<p>&lt;nodename&gt;/Supervisor Engine Group</p> <p><b>Note:</b> Only cards classified as Management Modules are considered for Card Redundancy Groups.</p>	HP ProCurve	<p>&lt;nodename&gt;/Management Module Group</p> <p><b>Note:</b> Only cards classified as Management Modules are considered for Card Redundancy Groups.</p>
Device Vendor	Naming Convention						
Cisco	<p>&lt;nodename&gt;/Supervisor Engine Group</p> <p><b>Note:</b> Only cards classified as Management Modules are considered for Card Redundancy Groups.</p>						
HP ProCurve	<p>&lt;nodename&gt;/Management Module Group</p> <p><b>Note:</b> Only cards classified as Management Modules are considered for Card Redundancy Groups.</p>						
Status	<p>Overall status for the current Card Redundancy Group. NNMi follows the ISO standard for status classification.</p> <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> The icons are displayed only in table views.</p>						
Status Last Modified	The date and time when the Status value was last modified.						

## Card Redundancy Group Form: Redundant Cards Tab

Card Redundancy Groups are configured to provide redundancy protection against processor card failures.

The "Card Redundancy Group Form" on the previous page provides details about the selected Card Redundancy Group.

**For information about each tab:**

### Redundant Group Member Cards

Attribute	Description
Redundant Cards	<p>Table of all of the cards that are members of this Card Redundancy Group. Use this table to access information about each card associated with the selected Card Redundancy Group.</p> <p>Double-click the row representing a Card. The "Card Form" on page 157 displays all details about the selected Card.</p> <p><b>Note:</b> Only parent cards can be members of this group, daughter cards are not permitted to participate in Card Redundancy Groups.</p>

## Card Redundancy Group Form: Incidents Tab

Card Redundancy Groups are configured to provide redundancy protection against processor card failures.

The "Card Redundancy Group Form" on the previous page provides details about the selected Card Redundancy Group.

**For information about each tab:**

### Incidents Associated with Cards in this Redundancy Group

Attribute	Description
Incidents	<p>Table of the Incidents associated with the selected Card Redundancy Group.</p> <p>These Incidents are sorted by creation time so that you can view the Incidents in chronological order. Use this table to determine which Incidents are still open for the selected Card Redundancy Group.</p> <p>Double-click the row representing an Incident. The "Incident Form" on page 311 displays all details about the selected incident.</p> <p><b>Tip:</b> See "Incident Form" on page 311 for more details about the incident attributes that appear in the incident table's column headings.</p>

## Card Redundancy Group Form: Status Tab

Card Redundancy Groups are configured to provide redundancy protection against processor card failures.

The "Card Redundancy Group Form" on page 204 provides details about the selected Card Redundancy Group.

**For information about each tab:**









### Card Redundancy Group Status History Table

Attribute	Description
Status History	<p>List of up to the last 30 changes in the status for the Card Redundancy Group. This table is useful for obtaining a summary of the Card Redundancy Group Status so that you can better determine any patterns in behavior and activity.</p> <p>Double-click the row representing a Status History. The "Card Redundancy Group Status History Form" below displays all details about the selected Status.</p>

## Card Redundancy Group Status History Form

Card Redundancy Group Status is derived from SNMP polling results for both cards in the Card Redundancy Group, as well as any conclusions. For information about how the current Status was determined, see the "Card Redundancy Group Form: Conclusions Tab" on the next page. Status reflects the most serious outstanding conclusion. See "Watch Status Colors" on page 285 for more information about possible status values.

### Status Attributes

Attribute	Description
Status	<p>Overall status for the current Card Redundancy Group. NNMi follows the ISO standard for status classification. Possible values are:</p> <ul style="list-style-type: none"><li> No Status</li><li> Normal (one Active card and one Standby card)</li><li> Disabled</li><li> Unknown</li><li> Warning</li><li> Minor</li><li> Major</li><li> Critical</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.

## Card Redundancy Group Form: Conclusions Tab

Card Redundancy Groups are configured to provide redundancy protection against processor card failures.

The "Card Redundancy Group Form" on page 204 provides details about the selected Card Redundancy Group.

**For information about each tab:**

### Outstanding Status Conclusion Values

Attribute	Description												
Outstanding Status Conclusions	<p>The dynamically generated list of summary statuses for the Card Redundancy Group that contributed to the current overall Status of the selected Card Redundancy Group. Status is set by the Causal Engine.</p> <p>Each Conclusion listed is outstanding and contributes to the current overall Status.</p> <p>This table is useful for obtaining a quick summary of the problem description for the current Card Redundancy Group that led up to the Card Redundancy Group's most current Status.</p> <p>The Status value is correlated based on the most critical Conclusions.</p> <p>Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion.</p> <p>The following table describes the possible Conclusions that might appear for a Card Redundancy Group object.</p> <p><b>Note:</b> A <b>Y</b> in the <b>Incident?</b> column indicates that the conclusion results in an incident.</p> <p><b>Critical Status Conclusions</b></p> <table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>CrgMultiplePrimary</td> <td>NNMi has identified multiple Primary Cards (for example, Card Active) in the Card Redundancy Group. This typically indicates the communication between the cards in the group is malfunctioning.</td> <td>Critical</td> <td>Y</td> </tr> <tr> <td>CrgNoPrimary</td> <td>NNMi is unable to identify a Primary Card (for example, Card Active) in the Card Redundancy Group. This typically indicates one of the following:               <ul style="list-style-type: none"> <li>One card, or both the Primary</li> </ul> </td> <td>Critical</td> <td>Y</td> </tr> </tbody> </table>	Conclusion	Description	Status	Incident?	CrgMultiplePrimary	NNMi has identified multiple Primary Cards (for example, Card Active) in the Card Redundancy Group. This typically indicates the communication between the cards in the group is malfunctioning.	Critical	Y	CrgNoPrimary	NNMi is unable to identify a Primary Card (for example, Card Active) in the Card Redundancy Group. This typically indicates one of the following: <ul style="list-style-type: none"> <li>One card, or both the Primary</li> </ul>	Critical	Y
Conclusion	Description	Status	Incident?										
CrgMultiplePrimary	NNMi has identified multiple Primary Cards (for example, Card Active) in the Card Redundancy Group. This typically indicates the communication between the cards in the group is malfunctioning.	Critical	Y										
CrgNoPrimary	NNMi is unable to identify a Primary Card (for example, Card Active) in the Card Redundancy Group. This typically indicates one of the following: <ul style="list-style-type: none"> <li>One card, or both the Primary</li> </ul>	Critical	Y										

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
		and Secondary Cards, are down. <ul style="list-style-type: none"> <li>• NNMi has identified only Secondary cards (for example Standby cards) in the group.</li> <li>• Communication between cards in the group is malfunctioning.</li> </ul>		
	<b>Warning Status Conclusions</b>			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
	CrgNoSecondary	A Card Redundancy Group does not have a secondary member. Neither card has a cardStandbyStatus equal to Standby. A properly functioning Card Redundancy Group should have one operational Primary Card and one operational Secondary Card.	Warning	Y
	<b>Unknown Status Conclusions</b>			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
	CrgUnmanagable	The SNMP Agent on the node hosting the Card Redundancy Group is not responding to SNMP queries.	Unknown	N
	<b>Normal Status Conclusions</b>			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
	CrgFailback	The initial Primary Card is now active. This conclusion can occur only when a failover has occurred and then the Card Redundancy Group has returned to its previous state.	Normal	N
	CrgNormal	The Card Redundancy Group is operating normally. It has one card operating as the Primary Card and the other acting as the Secondary Card.	Normal	N



### Outstanding Status Conclusion Values, continued

Attribute	Description			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
	CrgFailover	The Primary Card (for example, Card Active) has moved from one card to the other in a Card Redundancy Group. The Card Redundancy Group is routing packets properly.	Normal	Y






## 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.

**Note:** All members of a Router Redundancy Group must be assigned to the same Tenant (visible in the Node form's [Basic Attributes](#) and in the Tenants column of the [Inventory > Nodes view](#)). The NNMi administrator configures the Tenants.

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 <i>Active</i> or VRRP <i>Master</i> ).
Tenant	Tenants enable NNMi administrators to partition a network across multiple customers. The NNMi administrator controls the Tenant assignment for each Node. All Nodes in the Router Redundancy Group must be assigned to the same Tenant.  A Tenant is the top-level organization to which a n=Node belongs.
Status	Router Redundancy Group Status reflects the most serious Severity value of the incidents associated with the Router Redundancy Group. Possible values are:   Normal  Warning  Minor  Major  Critical

### Basics Attributes, continued

Attribute	Description
	See " <a href="#">Watch Status Colors</a> " on page 285 for more information about Severity values. <b>Note:</b> The icons are displayed only in table views.
Status Last Modified	Date and time indicating when the Status was last set.
Protocol	The protocol in use for the selected Router Redundancy Group. For example: Virtual Router Redundancy Protocol ( <a href="#">VRRP</a> <sup>1</sup> ) or Hot Standby Router Protocol ( <a href="#">HSRP</a> <sup>2</sup> ).
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 281](#)

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

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

**Note:** All members of a Router Redundancy Group must be assigned to the same Tenant (visible in the Node form's [Basic Attributes](#) and in the Tenants column of the [Inventory > Nodes view](#)). The NNMi administrator configures the Tenants.

For information about each tab:

### Router Redundancy Members in this Router Redundancy Group

Attribute	Description
Router Redundancy Members	Table of all of the routers that are members of the selected Router Redundancy Group. The table lists each router's interface that is associated with this Router Redundancy Group. Use this table to access information about each router.  Double-click the row representing a Router Redundancy Member. The " <a href="#">Router Redundancy Member Form (NNMi Advanced)</a> " on the next page displays all details about the selected Router Redundancy Member.

---

<sup>1</sup>Virtual Router Redundancy Protocol  
<sup>2</sup>Hot Standby Router Protocol



## 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 current 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	<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 hostname assigned to the router and the Name attribute value that NNMi 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: <code>HSRPRouter1.abc.example.com[Se1/1:1]</code></p> <p>See "Node Form" on page 50 for more information about node names. See "Interface Form" on page 90 for more information about interface names.</p>
Primary IP	<p>The IP Address used to exchange messages between routers in the Router Redundancy Group.</p>
Is Owner	<p>Boolean attribute used to Indicate whether the selected router owns a Virtual IP Address (if any) for the Router Redundancy Group. See "Virtual IP Addresses Form (NNMi Advanced)" on page 216 for more information.</p> <p>If the selected router uses a Router Redundancy Protocol that does not support virtual addresses, the value is set to <code>false</code>.</p>
Priority	<p>The configured protocol-specific number that indicates the current rank of the Router Redundancy Member.</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> Show Analysis to view the Analysis Pane information for the selected interface. (See "Use the Analysis Pane " on page 356 for more information</li></ul>

**Basics Attributes, continued**

Attribute	Description
	<p>about the Analysis Pane.)</p> <ul style="list-style-type: none"> <li>•  Open to open the Interface form.</li> </ul>
Hosted on Node	<p>Name attribute value from the "Node Form" on page 50 of the selected router (the Router Redundancy Group member).</p> <p>To find out more information about the Node:</p> <p>Click the  Lookup icon and choose one of the following options:</p> <ul style="list-style-type: none"> <li>•  Show Analysis to view the Analysis Pane information for the selected interface. (See "Use the Analysis Pane " on page 356 for more information about the Analysis Pane.)</li> <li>•  Open to open the Node form.</li> </ul>
Redundancy Group	<p>Name of the Router Redundancy Group to which the Router Redundancy Member belongs.</p> <p>To find out more information about the Router Redundancy Group:</p> <p>Click the  Lookup icon and choose one of the following options:</p> <ul style="list-style-type: none"> <li>•  Show Analysis to view the Analysis Pane information for the selected interface. (See "Use the Analysis Pane " on page 356 for more information about the Analysis Pane.)</li> <li>•  Open to open the Router Redundancy Group form.</li> </ul>
Current State	<p>State of the Router Redundancy Member. State values are protocol-specific. For example:</p> <ul style="list-style-type: none"> <li>• <b>Hot Standby Router Protocol (HSRP) States:</b>click here. <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>Standby</b> - Indicates the router is a candidate to become the next active router.</li> <li> <b>Initial</b> - Indicates <b>HSRP</b><sup>1</sup> 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 nor standby router. In this state, the router is waiting for a message from the active and standby routers.</li> </ul> </li> </ul>

<sup>1</sup>Hot Standby Router Protocol

### Basics Attributes, continued

Attribute	Description
	<ul style="list-style-type: none"> <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> <ul style="list-style-type: none"> <li>• <b>Virtual Router Redundancy Protocol (VRRP) States:</b>click here.</li> </ul> </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> <li>  <b>Initialize</b> - Indicates the router is not running VRRP protocol. This state occurs when an interface first comes up.         </li> </ul> <p>The following values indicate NNMi could not gather the required data:</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 this agent.         </li> <li>  <b>No Polling Policy</b> - Indicates the object is being polled, but no polling policy exists in Monitoring Configuration settings for this monitored attribute.         </li> <li>  <b>Not Polled</b> - Indicates that this 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. This object attribute might or might not have an associated polling policy.         </li> <li>  <b>Unavailable</b> - Unable to determine the State. For example, the SNMP agent returned a value outside the range of possible values or returned a null value.         </li> <li>  <b>Unset</b> – Currently not used by NNMi.         </li> <li>  <b>Other</b> – The SNMP agent responded with a value for the MIB variable used to determine the Router Redundancy Member State that is not recognized.         </li> </ul>
Previous State	The previous State of the Router Redundancy Member. State values are protocol-specific. For examples, see <a href="#">Current State</a> .
State Last Modified	Date and time the Router Redundancy State was last modified.

## 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 211 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:**

See "Tracked Objects Form (NNMi Advanced)" on the next page for more information about tracked objects.




**Tracked Objects Table**

Attribute	Description
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 hostname assigned to the router and the Name attribute value that NNMi 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]</i></p> <p>For example: HSRPRouter1.abc.example.com[Se1/1]</p> <p><b>Note:</b> NNMi determines this Name value. See "Node Form" on page 50 for more information about node names. See "Interface Form" on page 90 for more information about interface names.</p>
Track Priority	<p>Number NNMi uses to rank the tracked object whenever a <a href="#">Current State</a> change occurs. NNMi uses this number indirectly in the calculation to determine the next Primary member of the Router Redundancy Group.</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 Primary router in the Router Redundancy Group.</p> <p>For example, if an interface that has a Track Priority of 20 goes down on a Router Redundancy Member that has a member Priority of 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 Primary router in the group (for example, HSRP Active or VRRP Master).</li> </ul>
State Last Modified	<p>The date and time when the State value was last modified.</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
Name	<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><b>Note:</b> NNMi determines this Name value.</p> <p>The name includes the fully-qualified DNS hostname assigned to the router and the Name attribute value that NNMi 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]</i></p> <p>For example: <code>HSRPRouter1.abc.example.com[Se1/1]</code></p> <p>See "<a href="#">Node Form</a>" on page 50 for more information about node names. See "<a href="#">Interface Form</a>" on page 90 for more information about interface names.</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> Show Analysis to view the Analysis Pane information for the selected Tracked Object. (See "<a href="#">Use the Analysis Pane</a>" on page 356 for more information about the Analysis Pane.</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 that has a Track Priority of 20 goes down on a Router Redundancy Member that has a member Priority of 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</li> </ul>

### Basics Attributes, continued

Attribute	Description
	members in the Router Redundancy Group. <ul style="list-style-type: none"><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>
State Last Modified	Date and time the Tracked Object State was last modified.

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

The "Router Redundancy Group Form (NNMi Advanced)" on page 209 provides details about the selected Router Redundancy Group.

For information about each tab:

### Virtual IP Addresses Table

Attribute	Description
Virtual IP Addresses	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, VRRP Master). For each virtual IP address displayed, you can see the IP address value.  Double-click the row representing a Virtual IP Address. The " <a href="#">Virtual IP Addresses Form (NNMi Advanced)</a> " below displays all details about the selected Virtual 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, 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)

The "Router Redundancy Group Form (NNMi Advanced)" on page 209 provides details about the selected Router Redundancy Group.

For information about each tab:

### Incidents Associated with this Router Redundancy Group

Attribute	Description
Incidents	<p>Table of the Incidents associated with the selected Router Redundancy Group.</p> <p>These Incidents are sorted by creation time so that you can view the Incidents in chronological order. Use this table to determine which Incidents are still open for the selected Router Redundancy Group.</p> <p>Double-click the row representing an Incident. The "Incident Form" on page 311 displays all details about the selected incident.</p> <p><b>Tip:</b> See "Incident Form" on page 311 for more details about the incident attributes that appear in the incident table's column headings.</p>

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

The "Router Redundancy Group Form (NNMi Advanced)" on page 209 provides details about the selected Router Redundancy Group.

For information about each tab:

### Router Redundancy Group Status History Table









Attribute	Description
Status History	<p>List of up to the last 30 changes in the status for the Router Redundancy Group. This table is useful for obtaining a summary of the Router Redundancy status so that you can better determine any patterns in behavior and activity.</p> <p>Double-click the row representing a Status History. The "Router Redundancy Group Status History Form (NNMi Advanced)" below displays all details about the selected Status.</p>

## Router Redundancy Group Status History Form (NNMi Advanced)

Router Redundancy Group Status is derived from SNMP polling results, as well as any conclusions. For information about how the current Status was determined, see the "Router Redundancy Group Form: Conclusions Tab (NNMi Advanced)" on the next page. Status reflects

the most serious outstanding conclusion. See "Watch Status Colors" on page 285 for more information about possible status values.

### Status Attributes

Attribute	Description
Status	<p>Overall status for the current Router Redundancy Group. 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><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.

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

The "Router Redundancy Group Form (NNMi Advanced)" on page 209 provides details about the selected Router Redundancy Group.

All relevant conclusions are shown in the table on this tab. The most severe Status in the current group of conclusions becomes the overall Router Redundancy Group status:

**For information about each tab:**

### Outstanding Status Conclusion Values

Attribute	Description
Outstanding Status Conclusions	<p>The dynamically generated list of summary statuses for the Router Redundancy Group that contributed to the current overall Status of the selected Router Redundancy Group. Status is set by the Causal Engine.</p> <p>Each Conclusion listed is outstanding and contributes to the current overall Status.</p> <p>This table is useful for obtaining a quick summary of the problem description for the current Router Redundancy Group that led up to the Router Redundancy Group's most current Status.</p>

### Outstanding Status Conclusion Values, continued

Attribute	Description																								
	<p>The Status value is correlated based on the most critical Conclusions.</p> <p>Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion.</p> <p>The following table describes the possible Conclusions that might appear for a Router Redundancy object.</p> <p><b>Note:</b> A <b>Y</b> in the <b>Incident?</b> column indicates that the Conclusion results in an incident.</p> <p><b>Critical Status Conclusions</b></p> <table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>RrgNoPrimary</td> <td>           No primary device is identified in a Router Redundancy Group (for example, zero routers reporting HSRP Active or VRRP Master). This incident typically indicates one of the following:           <ul style="list-style-type: none"> <li>• Too many routers are down.</li> <li>• Protocol-specific communication between routers in the group is malfunctioning.</li> </ul> </td> <td>Critical</td> <td>Y</td> </tr> </tbody> </table> <p><b>Major Status Conclusions</b></p> <table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>RrgMultiplePrimary</td> <td>           Indicates that more than one router in a Router Redundancy Group is designated as Primary (for example, two routers reporting HSRP Active or VRRP Master). This incident typically indicates the protocol-specific communication between routers in the group is malfunctioning.         </td> <td>Major</td> <td>Y</td> </tr> </tbody> </table> <p><b>Minor Status Conclusions</b></p> <table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>RrgMultipleSecondary</td> <td>           Indicates that more than one secondary device is identified in a Router Redundancy Group (for example, HSRP Standby).         </td> <td>Minor</td> <td>Y</td> </tr> </tbody> </table>	Conclusion	Description	Status	Incident?	RrgNoPrimary	No primary device is identified in a Router Redundancy Group (for example, zero routers reporting HSRP Active or VRRP Master). This incident typically indicates one of the following: <ul style="list-style-type: none"> <li>• Too many routers are down.</li> <li>• Protocol-specific communication between routers in the group is malfunctioning.</li> </ul>	Critical	Y	Conclusion	Description	Status	Incident?	RrgMultiplePrimary	Indicates that more than one router in a Router Redundancy Group is designated as Primary (for example, two routers reporting HSRP Active or VRRP Master). This incident typically indicates the protocol-specific communication between routers in the group is malfunctioning.	Major	Y	Conclusion	Description	Status	Incident?	RrgMultipleSecondary	Indicates that more than one secondary device is identified in a Router Redundancy Group (for example, HSRP Standby).	Minor	Y
Conclusion	Description	Status	Incident?																						
RrgNoPrimary	No primary device is identified in a Router Redundancy Group (for example, zero routers reporting HSRP Active or VRRP Master). This incident typically indicates one of the following: <ul style="list-style-type: none"> <li>• Too many routers are down.</li> <li>• Protocol-specific communication between routers in the group is malfunctioning.</li> </ul>	Critical	Y																						
Conclusion	Description	Status	Incident?																						
RrgMultiplePrimary	Indicates that more than one router in a Router Redundancy Group is designated as Primary (for example, two routers reporting HSRP Active or VRRP Master). This incident typically indicates the protocol-specific communication between routers in the group is malfunctioning.	Major	Y																						
Conclusion	Description	Status	Incident?																						
RrgMultipleSecondary	Indicates that more than one secondary device is identified in a Router Redundancy Group (for example, HSRP Standby).	Minor	Y																						

**Outstanding Status Conclusion Values, continued**

Attribute	Description			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
		<p><b>Note:</b> This incident applies only to Router Redundancy Groups that allow only one secondary member. Typically, the protocol-specific communication between routers in the group is malfunctioning.</p> <p>Typically, the protocol-specific communication between routers in the group is malfunctioning.</p>		
	RrgNoSecondary	<p>Indicates that zero routers in a Router Redundancy Group are designated as Secondary (for example, no router reporting HSRP Standby or VRRP Backup).</p> <p>This incident typically indicates the following:</p> <ul style="list-style-type: none"> <li>• Protocol-specific communication between routers in the group is malfunctioning.</li> <li>• The group is routing packets properly because a single Primary device has been identified.</li> </ul>	Minor	Y
	<b>Warning Status Conclusions</b>			
	<b>Conclusion</b>	<b>Description</b>	<b>Status</b>	<b>Incident?</b>
	RrgGroupContainsUnmanagedMember	At least one, but not all SNMP Agents, associated with the member interfaces are not responding to	Warning	N

**Outstanding Status Conclusion Values, continued**

Attribute	Description		
	Conclusion	Description	Status Incident?
		SNMP queries or are not polled.	
	RrgDegraded	<p>This incident occurs only in Router Redundancy Groups with more than two members. This incident typically indicates the following:</p> <ul style="list-style-type: none"> <li>• The Router Redundancy Group has a Primary and Secondary device.</li> <li>• The remaining devices in the group are not in an expected protocol-specific state (for example, zero routers reporting HSRP Listen state).</li> <li>• Typically, the protocol-specific communication between routers is malfunctioning. However, the group is routing packets properly.</li> </ul>	Warning Y

### Outstanding Status Conclusion Values, continued

Attribute	Description																
	<p><b>Unknown Status Conclusions</b></p> <table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>RrgGroupAllMembersUnmanaged</td> <td>The SNMP Agent associated with all Router Redundancy Group member's interfaces are not responding to SNMP queries or are not polled.</td> <td>Unknown</td> <td>N</td> </tr> </tbody> </table> <p><b>Normal Status Conclusions</b></p> <table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>RrgOnePrimary</td> <td>At least one member of the Router Redundancy Group is acting as a Primary router.</td> <td>Normal</td> <td>N</td> </tr> </tbody> </table>	Conclusion	Description	Status	Incident?	RrgGroupAllMembersUnmanaged	The SNMP Agent associated with all Router Redundancy Group member's interfaces are not responding to SNMP queries or are not polled.	Unknown	N	Conclusion	Description	Status	Incident?	RrgOnePrimary	At least one member of the Router Redundancy Group is acting as a Primary router.	Normal	N
Conclusion	Description	Status	Incident?														
RrgGroupAllMembersUnmanaged	The SNMP Agent associated with all Router Redundancy Group member's interfaces are not responding to SNMP queries or are not polled.	Unknown	N														
Conclusion	Description	Status	Incident?														
RrgOnePrimary	At least one member of the Router Redundancy Group is acting as a Primary router.	Normal	N														

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

The "Router Redundancy Group Form (NNMi Advanced)" on page 209 provides details about a managed connection.

For information about each tab:

### Registration Attributes

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

### Object Identifiers Attributes

Attribute	Description
ID	The Unique Object Identifier, which is unique within the NNMi database.
UUID	The Universally Unique Object Identifier, which is unique across all databases.

## 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 for views](#). NNMi monitors the status of each Node Group over time. NNMi also provides a map of each Node Group (**Actions** → **Node Group Map**).

Each Node Group definition includes one or more of the following:

- Device Filters (by any combination of category, vendor, family, profile)
- Additional Filters (based on current object attribute values in the NNMi database)
- Additional Nodes (specific nodes identified by *case-sensitive* Hostname)
- Child Node Groups nest into this Node Group.

**For information about each tab:**

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

If you are an NNMi administrator, you can create Node Groups and 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). This name is a maximum of 255 characters. Alpha-numeric, spaces, and special characters (~ ! @ # \$ % ^ & * ( ) _ + -) are permitted.
Calculate Status	<i>NNMi Administrators only.</i> If disabled <input type="checkbox"/> , NNMi does not calculate the Status for this Node Group. NNMi sets the Node Group Status value to No Status.  If enabled <input checked="" type="checkbox"/> , NNMi calculates the Node Group Status according to the Status Configuration settings. See " <a href="#">Configure Node Group Status</a> " for more information.
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</a> " on page 230 for more information.
Add to View Filter List	<i>NNMi Administrators only.</i> 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

### Node Group Basic Settings, continued

Attribute	Description
	address, and incident views.
Notes	<p><i>Optional.</i> If your role permits, enter any information that might be useful to you and your team.</p> <p>Type a maximum of 1024 characters. Alpha-numeric, spaces, and special characters (~ ! @ # \$ % ^ &amp; * ( ) _ + -) are permitted.</p>

### Node Group Settings (NNM iSPI Performance)

Attribute	Description
Add to Filter List	<p><i>NNMi Administrators only.</i></p> <p>(<i>NNM iSPI Performance</i>) Using this feature is entirely optional. The NNM iSPI Performance software, such as HP Network Node Manager iSPI Performance for Metrics Software or HP Network Node Manager iSPI Performance for Traffic Software, 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 might 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 (*NNMi Administrators only*)

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

NNMi combines the results of all Node Group configuration settings in the following manner:

- NNMi first evaluates Device Filters. If any exist, nodes must match *at least one* specification to belong to this Node Group.
- NNMi then evaluates any Additional Filters. Nodes *must also pass all* Additional Filters specifications to belong to this Node Group.
- Any Additional Nodes specified are *always* included in the Node Group, regardless of any filters.
- Any Child Node Group results are treated the same as Additional Nodes.

The "Node Group Form" on the previous page 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>Double-click the row representing the node that has the "Node Device Filter Form (NNMi Administrators only)" below you want to see.</p>

## Node Device Filter Form (NNMi Administrators only)



*Optional:* Node Group definitions can specify membership using combinations of Device Profile attributes for device category, vendor, family, and profile. If you provide more than one Node Device Filter specification for a particular Node Group, the Node Group includes devices that pass any one of the Device Filters.

NNMi combines the results of all Node Group configuration settings in the following manner:




- NNMi first evaluates Device Filters. If any exist, nodes must match *at least one* specification to belong to this Node Group.
- NNMi then evaluates any Additional Filters. Nodes *must also pass all* Additional Filters specifications to belong to this Node Group.
- Any Additional Nodes specified are *always* included in the Node Group, regardless of any filters.
- Any Child Node Group results are treated the same as Additional Nodes.

Each Node Device Filter specifies one or more criteria that devices must meet to qualify for inclusion in the Node Group (see table below). If more than one criteria, devices must meet all of the criteria to pass that Node Device Filter and join the Node Group.

### 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.
Device Family	<i>Optional:</i> A particular family of devices. The drop-down list displays all available choices.
Device Profile	<p><i>Optional:</i> The text string for Device Model from the Device Profile.</p> <p><b>Tip:</b> According to industry standards (RFC 1213, MIB-II), each combination of vendor, category, and model is assigned a unique SNMP system object ID number (<b>sysObjectID</b>). NNMi provides a Device Profile for each of these. The Device Profile allows you to customize NNMi behavior for specific device models. If you want to know the actual SNMP system object ID number, use  Quick Find (see below).</p> <p>If your role permits, click the  Lookup icon and select one of the options from the</p>

**Device Attribute Filters Table , continued**

Attribute	Description
Device Category	<i>Optional:</i> A particular category of devices. The drop-down list displays all available choices.
	<p>drop-down menu:</p> <ul style="list-style-type: none"> <li>•  Show Analysis to view Analysis Pane information for the currently selected Device Profile. (See "Use the Analysis Pane " on page 356 for more information about the Analysis Pane.)</li> <li>•  Quick Find to view and select from the list of all existing Device Profiles.</li> <li>•  Open to display the details of the currently selected Device Profile.</li> <li>• * New to create a new Device Profile definition.</li> </ul>

## Node Group Form: Additional Filters Tab (NNMi Administrators only)

**Note:** The Additional Filters Editor requires that your user name be assigned a role of Administrator. If you are an NNMi Administrator, see [Specify Node Group Additional Filters](#) for more information about how to use the Additional Filters editor.

The Additional Filters tab enables the NNMi administrator to use expressions to refine the requirements for membership in a Node Group.

NNMi combines the results of all Node Group configuration settings in the following manner:

- NNMi first evaluates Device Filters. If any exist, nodes must match *at least one* specification to belong to this Node Group.
- NNMi then evaluates any Additional Filters. Nodes *must also pass all* Additional Filters specifications to belong to this Node Group.
- Any Additional Nodes specified are *always* included in the Node Group, regardless of any filters.
- Any Child Node Group results are treated the same as Additional Nodes.

The "Node Group Form" on [page 223](#) 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 (NNMi Administrators only)

*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 223 provides details about the selected node group.

For information about each tab:

### Specific-Device Filters Table

Attribute	Description
Node Hostname	Table view of the <i>case-sensitive</i> Hostnames for the additional nodes added as members of the selected Node Group.  Double-click the row representing the node that has the "Additional Node Form (NNMi Administrators only)" below you want to see.

## Additional Node Form (NNMi Administrators only)

*Optional:* Node Group definitions can specify members by *case-sensitive* Hostname (on the "Node Group Form: Additional Nodes Tab (NNMi Administrators only)" on the previous page).

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

**Tip for Administrators:** To add more than a few additional nodes to the Node Group, create a Custom Attribute for the nodes. Use the Additional Filters tab with the Custom Attribute value to group the nodes together. See "Node Form: Custom Attributes Tab" on page 68 and "Node Custom Attributes Form" on page 68 for more information.

### Specific Node Group Member

Attribute	Description
Node Hostname	<p>The current value of the <i>fully-qualified, case-sensitive</i> Hostname attribute as it appears on the Node form.</p> <p>NNMi follows a set of rules to dynamically generate the value stored in the NNMi database for each Node's Hostname. Click here for details.</p> <ul style="list-style-type: none"> <li>• If the Node supports SNMP, NNMi requests the Hostname using the IP Address of the associated SNMP agent (the Management Address attribute value on the Node form).</li> </ul> <p>When the NNMi administrator chooses <b>Enable SNMP Address Rediscovery</b> <input checked="" type="checkbox"/> in the Communication Configuration:</p> <ul style="list-style-type: none"> <li>▪ If the SNMP Agent does not respond, NNMi checks for another Management Address to request the Hostname, and the Hostname could change.</li> <li>▪ If the SNMP Agent associated with the node changes, the Management Address and Hostname could change.</li> </ul> <p>When the NNMi administrator disables <b>Enable SNMP Address Rediscovery</b> <input type="checkbox"/> in the Communication Configuration:</p> <ul style="list-style-type: none"> <li>▪ If the SNMP Agent does not respond, NNMi uses the previously gathered Management Address attribute value to request the Hostname.</li> <li>▪ If the SNMP Agent associated with the node changes, NNMi uses the previously gathered Management Address attribute value to request the</li> </ul>

### Specific Node Group Member, continued


Attribute	Description
	<p>Hostname.</p> <ul style="list-style-type: none"><li>If the Node does not support SNMP, no Management Address is available. NNMI requests a Hostname starting with the lowest IP Address associated with the node (a Discovery Seed value or an IP address value gathered from a neighboring device). NNMI uses the first Hostname provided. The Hostname might change during a future discovery cycle.</li></ul> <p><b>Note:</b> NNMI administrators can use NNMI property file settings to change the way NNMI determines Hostname values:</p> <ul style="list-style-type: none"><li><code>nms-topology.properties</code> file settings: If DNS is the source of the Node's Hostname, there are three choices. By default NNMI uses the exact Hostname from your network configuration. It is possible to change NNMI behavior to convert Hostnames to all uppercase or all lowercase. See the "Modifying NNMI Normalization Properties" section of the <i>HP Network Node Manager i Software Deployment Reference</i>, which is available at: <a href="http://h20230.www2.hp.com/selfsolve/manuals">http://h20230.www2.hp.com/selfsolve/manuals</a>.</li><li><code>nms-disco.properties</code> file settings: The Hostname is either requested from the Node's lowest loopback interface IP address that resolves to a Hostname or requested from the Node's designated Management Address (SNMP agent address). With either choice, when no IP address resolves to a Hostname, the IP address itself becomes the Hostname. See the "Maintaining NNMI" chapter of the <i>HP Network Node Manager i Software Deployment Reference</i>, which is available at: <a href="http://h20230.www2.hp.com/selfsolve/manuals">http://h20230.www2.hp.com/selfsolve/manuals</a>.</li></ul> <p>See "Access Node Details" on page 287 and <a href="#">Access More Details (Forms and Analysis Pane)</a> for a description of the ways to verify node details.</p>

## Node Group Form: Child Node Groups Tab (NNMI Administrators only)

The "Node Group Form" on page 223 provides details about the selected Node Group.

A set of Node Groups can be hierarchically configured, for example, based on geographical location. The *Parent* Node Group might be named **North America** to represent all of the nodes on that continent. Additional Node Groups might exist for each country in which your business offices reside (for example **Canada**, **Mexico** and **United States**). Each of these individual Node Groups are configured as a *Child* Node Group of the **North America** Node Group.

For information about each of the columns displayed in the Child Node Groups table, see "Node Group Hierarchy (Child Node Group) Form (NNMI Administrators only)" on the next page.

By default, each *Child* Node Group is represented by a  hexagon symbol 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.

Alternatively, an NNMI administrator 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 (NNMI Administrators only)" below for more information.

**For information about each tab:**

**Related Topics**

"Node Group Maps" on page 253

"Navigating within a Node Group Map" on page 256

"Position Nodes on a Node Group Map" on page 257

## Node Group Hierarchy (Child Node Group) Form (NNMI Administrators only)


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	<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>
Expand Child in Parent Node Group Map	<p>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.</p> <p>If enabled, each node in the group appears as a separate node on the Node Group Map.</p> <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</li> </ul>

### Basics Attributes, continued

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>
	<p>hexagon as shown below:</p>  <ul style="list-style-type: none"><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>Expand</b> column in the <b>Child Node Groups</b> table view.</p>

#### Related Topics

["Node Group Maps" on page 253](#)



["Position Nodes on a Node Group Map" on page 257](#)

## Node Group Form: Status Tab








NNMi calculates the Node Group status based on the status of the nodes within the group. NNMi follows the ISO standard for status classification. Your NNMi administrator chooses a strategy for calculating Node Group Status. Possible strategies are:

- Propagating the Most Severe Status
- Configuring percentage thresholds

By default, NNMi uses the strategy for Propagating the Most Severe Status. NNMi sets the Node Group status equal to the most severe Status of any node in the Node Group.

NNMi can also use the alternative Percentage threshold strategy. NNMi sets the Node Group status according to rules defined by your NNMi Administrator. When more than one Status percentage exceeds the threshold, NNMi propagates the most severe status. For example using the settings below, if the percentage of nodes with  **Warning** Status exceeds 30 percent and the number of nodes with  **Minor** Status exceeds 20 percent, NNMi assigns the Node Group a Status of Minor.

The following list shows an example of using the alternative Percentage strategy:








-  **No Status** — The Node Group has just been added and NNMi has not yet calculated the status.
-  **Normal** — All nodes in the Node Group have a status of Normal or the threshold specified for this Target Status has not been reached.
-  **Unknown** — All nodes within the Node Group have a status of **Unknown**.
-  **Warning** — At least 30 percent of the nodes within the Node Group have a status of **Warning**.
-  **Minor** — At least 20 percent of the nodes in the Node Group have a Status of **Minor**.
-  **Major** — At least 10 percent of the nodes within the Node Group have a status of **Major**.
-  **Critical** — At least 5 percent of the nodes in the group have a status of **Critical**.

**Note:** These example percentages might not match your NNMi Administrator's choices. See "Help for Administrators" for more information.

The "Node Group Form" on page 223 provides details about the selected Node Group.

**For information about each tab:**

**Status Attributes**

Attribute	Description
Status	<p>NNMi calculates the Node Group status based on the status of the nodes within the group. Your NNMi administrator chooses a strategy for calculating Node Group Status. Possible strategies are:</p> <ul style="list-style-type: none"> <li>• Propagating the Most Severe Status (NNMi default setting)</li> <li>• Configuring percentage thresholds</li> </ul> <p>Possible status values are as follows. See "Watch Status Colors" on page 285 for more information about the meaning of possible status values. The status icons are displayed in table views. All other locations use status colors (instead of icons):</p> <div style="display: flex; justify-content: space-around; align-items: flex-start;"> <div style="text-align: center;">  <b>No Status</b> </div> <div style="text-align: center;">  <b>Unknown</b> </div> <div style="text-align: center;">  <b>Minor</b> </div> </div> <div style="display: flex; justify-content: space-around; align-items: flex-start; margin-top: 10px;"> <div style="text-align: center;">  <b>Normal</b> </div> <div style="text-align: center;">  <b>Warning</b> </div> <div style="text-align: center;">  <b>Major</b> </div> </div> <div style="display: flex; justify-content: center; align-items: center; margin-top: 10px;">  <b>Critical</b> </div>
Status Last Modified	Date and time indicating when the status was last set.

**Status History Table**

Attribute	Description
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

### Status History Table, continued

Attribute	Description
	patterns in behavior and activity.  Double-click the row representing a Status History. The Status History form displays all details about the selected 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.

The NNMi administrator can create and modify Interface Group definitions. The NNMi administrator can also configure [Interface Groups as filters for views](#).

When determining membership in this Interface Group, NNMi combines the results of all Interface Group configuration settings in the following manner:

- NNMi first evaluates ifType Filters. If any exist, interfaces must match *at least one* specification to belong to this Interface Group.
- NNMi then evaluates any Additional Filters. Interfaces *must also pass all* Additional Filters specifications to belong to this Interface Group.
- If a Node Group is specified for this Interface Group, any interface in this group must be contained in a node that is a member of the Node Group specified in the Basics section.

#### For information about each tab:

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

If you are an NNMi administrator, you can create Interface Groups and use Interface Groups in several ways:

### Interface Group Basics

Attribute	Description
Name	The name of this group (text string specified by the NNMi administrator). This name is a maximum of 255 characters. Alpha-numeric, spaces, and special characters (~ ! @ # \$ % ^ & * ( ) _ + -) are permitted.
Add to View Filter List	If disabled <input type="checkbox"/> , this interface group does not appear in any interface group filter lists for interface and IP address views.  If enabled <input checked="" type="checkbox"/> , this interface group is a filter for all interface and IP address views.
Node Group	<i>Optional.</i> If configured, the specified Node Group serves as a filter for this Interface Group.  If you specify a Node Group, any interface in this group must be contained in a node



### Interface Group Basics , continued

Attribute	Description
	that matches the specified Node Group. For example, an Interface Group configured for Ethernet-only interfaces could be further refined by associating a Node Group configured for Printers-only. You could then gather data about all printers that contain Ethernet interfaces.
Notes	<p><i>Optional.</i> If your role permits, enter any information that might be useful to you and your team.</p> <p>Type a maximum of 1024 characters. Alpha-numeric, spaces, and special characters (~ ! @ # \$ % ^ &amp; * ( ) _ + -) are permitted.</p>

### NNM iSPI Performance

Attribute	Description
Add to Filter List	<p><i>(NNM iSPI Performance)</i> Using this feature is entirely optional. The NNM iSPI Performance software, such as HP Network Node Manager iSPI Performance for Metrics Software or HP Network Node Manager iSPI Performance for Traffic Software, 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 might 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.

When determining membership in this Interface Group, NNMi combines the results of all Interface Group configuration settings in the following manner:

- NNMi first evaluates ifType Filters. If any exist, interfaces must match *at least one* specification to belong to this Interface Group.
- NNMi then evaluates any Additional Filters. Interfaces *must also pass all* Additional Filters specifications to belong to this Interface Group.
- If a Node Group is specified for this Interface Group, any interface in this group must be contained in a node that is a member of the Node Group specified in the Basics section.

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

**For information about each tab:**



### ifType Filters Table

Attribute	Description
ifType Filters	Table view of all ifType filters associated with the selected interface group. If the Security configuration permits, double-click the row representing the ifType filter to view more details on the "ifType Filter Form" below.

## ifType Filter Form

If the NNMi Security configuration permits access to this 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	Click the  Lookup icon and select  Open to display the "ifType (Interface Type) Form" below and view more information about the specified IANA ifType-MIB variable.  If your role permits, you can easily choose from a list of all known industry-standard IANAifType-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> )

## 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	Text string. The IANA ifType TEXTUAL-CONVENTION values extracted from the IANA ifType-MIB. This text string displays as the ifType 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> )  If your role permits, click the  Lookup icon and select one of the options from the drop-down menu: <ul style="list-style-type: none"><li> Show Analysis to view Analysis Pane information for the currently selected ifType. (See "Use the Analysis Pane " on page 356 for more information about the Analysis Pane.)</li><li> Quick Find to view and select from the list of all available ifType values.</li></ul>

### Interface Type Definition, continued

Attribute	Description
	<ul style="list-style-type: none"><li>📁 Open to display the details of the currently selected <code>ifType</code>.</li><li>✳️ New to create a new <code>ifType</code> definition.</li></ul>
Number	Industry-standard number assigned to this <code>ifType</code> value.
Description	<p><i>Optional.</i> If your role permits, provide any description that would be useful for communication purposes within your team.</p> <p>Type a maximum of 2048 characters. Alpha-numeric, spaces, and special characters (~ ! @ # \$ % ^ &amp; * ( ) _ + -) are permitted.</p>

## Interface Group Form: Additional Filters Tab

**Note:** To *create* Additional Filters, your user name must be assigned to the role of NNMI Administrator.

Additional Filters enable the NNMI administrator to create expressions that further refine which interfaces to include in an Interface Group. If an NNMI administrator created any Additional Filters for the selected Interface Group, NNMI displays the Additional Filters expression. See [Specify Interface Group Additional Filters](#) for information about how to use the Additional Filters Editor or how to decipher an existing Additional Filters expression.

When determining membership in this Interface Group, NNMI combines the results of all Interface Group configuration settings in the following manner:

- NNMI first evaluates `ifType` Filters. If any exist, interfaces must match *at least one* specification to belong to this Interface Group.
- NNMI then evaluates any Additional Filters. Interfaces *must also pass all* Additional Filters specifications to belong to this Interface Group.
- If a Node Group is specified for this Interface Group, any interface in this group must be contained in a node that is a member of the Node Group specified in the Basics section.

The "Interface Group Form" on [page 232](#) provides details about the selected Interface Group.

**For information about each tab:**

## MPLS WAN Cloud (RAMS) Form (NNMi Advanced)

The MPLS WAN Cloud (RAMS) form provides information for the selected MPLS WAN Cloud. The following table describes the fields included on the MPLS WAN Cloud (RAMS) form:

### Basic Attributes

Attributes	Description
MPLS WAN Cloud	The name assigned to the discovered MPLS WAN Cloud.

**Basic Attributes, continued**

Attributes	Description
Name	
AS Number	The Autonomous System Number assigned to the MPLS WAN Cloud.
CEs	The number of Customer Edge (CE) routers associated with the MPLS WAN Cloud.

**Related Topics:**

"MPLS WAN Cloud (RAMS) Form: MPLS WAN Connections Tab (NNMi Advanced)" below









"MPLS WAN Cloud Map (NNMi Advanced)" on page 271

## MPLS WAN Cloud (RAMS) Form: MPLS WAN Connections Tab (NNMi Advanced)

The "MPLS WAN Cloud Form" provides details about the selected MPLS VPN Cloud.

**Note:** The Last Discovered Time is displayed in the MPLS WAN Interface summary. It is the date and time when the selected MPLS WAN Cloud was last discovered.

**Basic Attributes**

Attributes	Description
CE Status	Overall status for the Customer Edge (CE <sup>1</sup> ) router. The possible values are:  No Status  Normal  Disabled  Unknown  Warning  Minor  Major  Critical
CE Name	The name assigned to the CE router.
CE Interface	Interface of the CE router participating in the MPLS WAN Cloud.

<sup>1</sup>Customer Edge router. The router in your network that sends data to an Internet Service Provider's router (the Provider Edge) on the path to the data's final destination.

### Basic Attributes, continued

Attributes	Description
CE Address	The IP address of the CE router.
PE Address	The IP address of the Provider Edge (PE <sup>1</sup> ) router.
Protocol	The routing protocol used between the CE and the PE router.

#### Related Topics:

"MPLS WAN Cloud Map (NNMi Advanced)" on page 271

## Custom Node Collections Form




The Custom Node Collections form provides details about the Custom Node Collection you selected from the Monitoring workspace. A Custom Node Collection identifies a topology node that has at least one associated Custom Poller Policy. Because a topology node can be associated with more than one Policy, the same topology node might appear in multiple Custom Node Collections.

The following table describes the attributes included on the Custom Node Collection form.

The Custom Node Collections form also provides details about the [Status](#), [Conclusions](#), and [Polled Instances](#) associated with this Custom Poller Node.









#### For information about each tab:

#### Basic Attributes

Attribute	Description
Node	<p>Name of the topology node from which the Custom Poller Policy information is being collected. This is the current value in the NNMi database for the Name attribute of the node. 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  Show Analysis or  Open to display more information about the node.</p>
Active State	<p>The Active State for the associated Custom Collect Policy. Possible values are described below:</p> <p><b>Active</b> - Indicates the Custom Poller Policy is in use.</p> <p><b>Note:</b> At the time the Active State attribute is set to <b>Active</b>, NNMi applies the Custom Poller Policy to the nodes in the specified Node Group to determine which instances should be polled.</p> <p><b>Inactive</b> - Indicates the Custom Poller Policy is not in use. NNMi removes all</p>

<sup>1</sup>Provider Edge router. The Internet Service Provider's router that receives your data on the path to your data's final destination. The Customer Edge (CE) router in your network connects to this PE.

### Basic Attributes, continued

Attribute	Description
	<p>Polled Instances associated with the Policy.</p> <p><b>Suspended</b> - Indicates someone on your team changed this Custom Poller Policy's <i>Active State</i> to <i>Suspended</i>, or the NNMi administrator disabled Custom Poller in the <i>Global Control</i> settings of <b>Configuration</b> workspace, <b>Custom Poller Configuration</b> form. NNMi suspends polling and retains the most recent State value from before the Policy was suspended.</p>
Status	<p>The most severe State value returned from the Custom Poller Polled Instances for this Custom Node Collection.</p> <p>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>
Policy	<p>A Policy specifies the Node Group and Polling Interval that NNMi should use when polling the results of the MIB Expression configured for the current Custom Poller Collection.</p> <p>If the NNMi Security configuration permits, click the  Lookup icon and select  Show Analysis or  Open to display more information about the current Custom Poller Node's Policy.</p>
Discovery State	<p>Indicates the progress toward collecting data associated with this <a href="#">Polled Instance</a> (discovery using the MIB Expression objects for which you are collecting information). Possible values include:</p> <p><b>Created</b> - NNMi has not yet discovered any data for this new Polled Instance.</p> <p><b>In progress</b> - NNMi is currently collecting data for this Polled Instance.</p> <p><b>Completed</b> - NNMi gathered the data associated with this Polled Instance and placed it in the NNMi database.</p> <p><b>Unresponsive</b> - The SNMP agent did not respond when NNMi attempted to gather the data associated with this Polled Instance.</p> <p><b>Failed</b> - NNMi is unable to gather the data associated with this Polled Instance. Look in the Discovery State Information field for details.</p>
Discovery State Last Modified	<p>The date and time when the Discovery State value was last modified.</p>
Discovery	<p>Indicates any problems contributing to the Discovery State calculation.</p>

### Basic Attributes, continued

Attribute	Description
State Information	

### Related Topics

"About Custom Poller"

## Custom Node Collections Form: Incidents Tab

Tip: The "Custom Node Collections Form" on page 237 provides details about the selected Custom Node Collection.

**For information about each tab:**

### Incidents Table






Description
Table view of the incidents associated with the selected Custom Node Collection. 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 Custom Node Collection.  To see more information about an incident, double-click the row representing an incident. The "Incident Form" on page 311 displays all details about the selected incident.

## Custom Node Collections Form: Status Tab

The "Custom Node Collections Form" on page 237 provides details about the selected Custom Node Collection.

**For information about each tab:**

### Overall Status

Attribute	Description
Status	The most severe value returned from the Polled Instances for this Custom Node Collection.  Possible values are: <ul style="list-style-type: none"><li> Normal</li><li> Warning</li><li> Minor</li><li> Major</li><li> Critical</li></ul>
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 Custom Node Collection. This view is useful for obtaining a summary of the Custom Node Collection Status so that you can better determine any patterns in node behavior and activity.</p> <p>Double-click a row representing a Status History. The Status History form displays all details about the selected Status.</p>

## Custom Node Collections Form: Conclusions Tab

**Tip:** The "Custom Node Collections Form" on page 237 provides details about the selected Custom Node Collection.

For information about each tab:

### Outstanding Status Conclusion Values

Attribute	Description								
Outstanding Status Conclusions	<p>The dynamically generated list of summary statuses of the Custom Node Collection that contributed to the current overall Status of the selected Custom Node Collection.</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 that led up to the Custom Node Collection's most current Status.</p> <p>The Status value is correlated based on the most critical outstanding Conclusions.</p> <p>Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion.</p> <p>The following table describes the possible Conclusions that might appear for a Custom Node Collection object.</p> <p><b>Note:</b> A Y in the <b>Incident?</b> column indicates that the Conclusion results in an incident.</p> <p><b>Critical Status Conclusions</b></p> <table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>CustomPollCritical</td> <td>A Custom Polled Instance associated with the Custom Poller Collection is in a Critical State.</td> <td>Critical</td> <td>Y</td> </tr> </tbody> </table> <p><b>Major Status Conclusions</b></p>	Conclusion	Description	Status	Incident?	CustomPollCritical	A Custom Polled Instance associated with the Custom Poller Collection is in a Critical State.	Critical	Y
Conclusion	Description	Status	Incident?						
CustomPollCritical	A Custom Polled Instance associated with the Custom Poller Collection is in a Critical State.	Critical	Y						



### Outstanding Status Conclusion Values, continued

Attribute	Description								
	<table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>CustomPollMajor</td> <td>A Custom Polled Instance associated with the Custom Poller Collection is in a Major State.</td> <td>Major</td> <td>Y</td> </tr> </tbody> </table>	Conclusion	Description	Status	Incident?	CustomPollMajor	A Custom Polled Instance associated with the Custom Poller Collection is in a Major State.	Major	Y
Conclusion	Description	Status	Incident?						
CustomPollMajor	A Custom Polled Instance associated with the Custom Poller Collection is in a Major State.	Major	Y						
	<p><b>Minor Status Conclusions</b></p> <table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>CustomPollMinor</td> <td>A Custom Polled Instance associated with the Custom Poller Collection is in a Minor State.</td> <td>Minor</td> <td>Y</td> </tr> </tbody> </table>	Conclusion	Description	Status	Incident?	CustomPollMinor	A Custom Polled Instance associated with the Custom Poller Collection is in a Minor State.	Minor	Y
Conclusion	Description	Status	Incident?						
CustomPollMinor	A Custom Polled Instance associated with the Custom Poller Collection is in a Minor State.	Minor	Y						
	<p><b>Warning Status Conclusions</b></p> <table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>CustomPollWarning</td> <td>A Custom Polled Instance associated with the Custom Poller Collection is in a Warning State.</td> <td>Warning</td> <td>Y</td> </tr> </tbody> </table>	Conclusion	Description	Status	Incident?	CustomPollWarning	A Custom Polled Instance associated with the Custom Poller Collection is in a Warning State.	Warning	Y
Conclusion	Description	Status	Incident?						
CustomPollWarning	A Custom Polled Instance associated with the Custom Poller Collection is in a Warning State.	Warning	Y						
	<p><b>Normal Status Conclusions</b></p> <table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>CustomPollNormal</td> <td>A Custom Polled Instance associated with the Custom Poller Collection is in a Normal State.</td> <td>Normal</td> <td>N</td> </tr> </tbody> </table>	Conclusion	Description	Status	Incident?	CustomPollNormal	A Custom Polled Instance associated with the Custom Poller Collection is in a Normal State.	Normal	N
Conclusion	Description	Status	Incident?						
CustomPollNormal	A Custom Polled Instance associated with the Custom Poller Collection is in a Normal State.	Normal	N						

## Custom Node Collections Form: Polled Instances Tab

Tip: The "Custom Node Collections Form" on page 237 provides details about the selected Custom Node Collection.

For more information about Custom Polled Instances, click [here](#).

The first time a MIB Expression is validated with discovery information, the results appear in the **Monitoring** workspace's [Custom Polled Instances](#) view.

Each Custom Polled Instance:

- Updates whenever a change in State occurs (defined using [Threshold](#) or [Comparison Maps](#) settings).
- Includes the most recent polled *value* that caused the State to change.

These results are then used to determine the Status of the associated Custom Node Collection.

For example, you can specify that each time the `hrDeviceStatus` for a COM (communication) port returns a value of **5 (down)**, the State of the Polled Instance becomes **Critical**, which automatically affects the Status of the associated Custom Node Collection.

**For information about each tab:**

**Polled Instances Table**

Attribute	Description
Polled Instances List	<p>Information about Custom Poller Policy information being collected.</p> <p>This table is useful for obtaining a quick summary.</p> <p>Double-click the row representing a Polled Instance. The "<a href="#">Custom Polled Instance Form</a>" below displays all details about the selected Polled Instance.</p>

## Custom Polled Instance Form

The [Custom Polled Instance](#)<sup>1</sup> form provides details about the Custom Polled Instance you selected from the **Monitoring** workspace. The following table describes the attributes included on the Polled Instance form.

*(NNMi Advanced - Global Network Management feature)* Any Custom Polled Instances are not sent from a Regional Manager (NNMi management server) to the Global Manager. From the Global Manager, use **Actions** → **Open from Regional Manager** to see the list of Custom Polled Instances on the Regional Manager.

**For information about each tab:**

Note the following about Custom Polled Instances:










- The first time a MIB Expression is validated with discovery information, the results appear in the **Monitoring** workspace's [Custom Polled Instances view](#).
- Each Custom Polled Instance:
  - Updates whenever a change in State occurs (defined using [Threshold](#) or [Comparison Maps](#) settings).
  - Includes the most recent polled *value* that caused the State to change.
- These results are then used to determine the Status of the associated Custom Node Collection.

For example, you can specify that each time the `hrDeviceStatus` for a COM (communication) port returns a value of **5 (down)**, the State of the Polled Instance becomes **Critical**, which automatically affects the Status of the associated Custom Node Collection.











---

<sup>1</sup>A Custom Polled Instance represents the results of a MIB expression when it is evaluated against a node. The first time a MIB Expression is validated with discovery information, the results appear in the Monitoring workspace's Custom Polled Instances view. The Custom Polled Instance is updated whenever a change in State occurs and includes the most recent polled value that caused the State to change. These results are then used to determine the Status of the associated Custom Node Collection.

### Basic Attributes

Attribute	Description
Node	<p>Name of the topology node on which the Custom Poller Policy information is being collected. This is the current value in the NNMi database for the Name attribute of the node. 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  Show Analysis or  Open to display more information about the topology node.</p>
MIB Instance	<p>This attribute contains the multiple filtered instances for the MIB Expression. Each instance value identifies a row in the MIB table.</p> <p><b>Note:</b> If a MIB Expression includes multiple MIB Variables that have multiple instances, each instance value that is valid across all MIB Variables for a node is listed here. If NNMi is unable to find the same instance for all MIB Variables in the expression, a Polled Instance is not created. This is because NNMi cannot correctly evaluate a MIB Expression with missing values. If Polled Instances are not created as expected, check the Custom Node Collection view for Discovery State and Discovery State Information values.</p>
Filter Value	The instance of a MIB Variable value after the MIB Filter is applied.
Display Attribute	<p>The MIB Variable that contains the values NNMi displays when generating Custom Polled Instance or Line Graph results.</p> <p><b>Note:</b> The NNMi administrator selects this <b>Display Variable</b> when configuring the MIB Expression for a Custom Poller Collection.</p>
Active State	Specifies whether a Custom Poller Policy is enabled.
Custom Node Collection	<p>Name of the associated Custom Node Collection. A Custom Node Collection identifies a topology node that has at least one associated Custom Poller Policy. Because a topology node can be associated with more than one Policy, the same topology node might appear in multiple Custom Node Collections.</p> <p>Click the  Lookup icon and select  Show Analysis or  Open to display more information about the Custom Node Collection.</p> <p>See "<a href="#">Custom Node Collections Form</a>" on page 237 for more information.</p>
Custom Poller Policy	Name of the associated Custom Poller Policy. The Custom Poller Policy defines the Node Group from which the MIB information is polled.
Custom Poller Collection	<p>Name of the Custom Poller Collection. A Custom Poller Collection defines the information you want to gather (poll) as well as how you want NNMi to handle the results.</p> <p>Click the  Lookup icon and select  Show Analysis or  Open to display more information about the Custom Poller Collection.</p>

**Basic Attributes, continued**

Attribute	Description
	See "Custom Polled Collection Form" on page 247 for more information.
Status	<p>Overall status for the current Custom Polled Instance. NNMi follows the ISO standard for status classification. See the "Custom Polled Instance Form: Status Tab" on the next page for more information. 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>Status reflects the most serious outstanding conclusion. See "Watch Status Colors" on page 285 for more information about possible status values.</p> <p><b>Note:</b> The icons are displayed only in table views</p>
State	<p>The State of the Custom Polled Instance as determined by any Thresholds (<a href="#">High State / Low State</a> value) or Comparison Maps (State Mapping = the NNMi administrator assigns a State value for each possible Polled Instance value) configured for the current Custom Poller Collection's MIB Expression.</p> <p>Possible State values for a <i>Polled Instance</i> (Threshold = High State/Low State; or Comparison Map = State Mapping) 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><b>Note:</b> The most severe Threshold <a href="#">High State</a> or <a href="#">Low State</a> value or Comparison Map <i>State Mapping</i> value returned from the Polled Instances for a <a href="#">Custom Node Collection</a> becomes the Custom Node Collection Status.</p>
Last State Change Value	<p>The value from the MIB Expression that most recently caused the State to change.</p> <p><b>Note:</b> A value of <b>null</b> indicates that a value was unavailable or an error occurred while evaluating the MIB Expression.</p>
State Last Modified	The date and time the Polled Instance was last modified.

## Custom Polled Instance Form: Incidents Tab

**Tip:** The "Custom Polled Instance Form" on page 242 provides details about the selected Custom Polled Instance.

The Name of the Source Object for a Custom Polled Instance Incident is the display value that is determined using the Instance Display Configuration for the associated MIB Expression.

If the Instance Display Configuration is not set, NNMi identifies the Source Object using the topology Node Name followed by the MIB Instance value in the format: `<node_name> -.<MIB_instance_value>`.

**Note:** The Name that NNMi uses to identify the Custom Polled Instance Incident's Source Object is not stored in the NNMi database as the Custom Polled Instance object Name.

**For information about each tab:**

### Incidents Table






Description
Table view of the incidents associated with the selected Custom Polled Instance. These incidents are sorted by creation time so that you can view the incidents in chronological order. Use this view to determine which incident is still open for the selected Custom Polled Instance.
To see more information about an incident, double-click the row representing an incident. The "Incident Form" on page 311 displays all details about the selected incident.

## Custom Polled Instance Form: Status Tab

The "Custom Polled Instance Form" on page 242 provides details about the selected Custom Polled Instance.

**For information about each tab:**

### Overall Status

Attribute	Description
Status	The most severe value returned from the Custom Polled Instance. Possible values are:  Normal  Warning  Minor  Major  Critical
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 Custom Polled Instance. This view is useful for obtaining a summary of the Custom Polled Instance Status so that you can better determine any patterns in node behavior and activity.</p> <p>Double-click a row representing a Status History. The Status History form displays all details about the selected Status.</p>

## Custom Polled Instance Form: Conclusions Tab

**Tip:** The "Custom Polled Instance Form" on page 242 provides details about the selected Custom Polled Instance.

**For information about each tab:**

### Outstanding Conclusions Table

Attribute	Description								
Outstanding Status Conclusions	<p>The dynamically generated list of summary statuses of the Custom Polled Instance that contributed to the current overall Status of the selected Custom Polled Instance.</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 that led up to the Custom Polled Instances most current Status.</p> <p>The Status value is correlated based on the most critical outstanding Conclusions.</p> <p>Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion.</p> <p>The following table describes the possible Conclusions that might appear for a Custom Polled Instance object.</p> <p><b>Note:</b> A <b>Y</b> in the <b>Incident?</b> column indicates that the Conclusion can result in an incident. An NNMi administrator can configure whether incidents are generated. See <a href="#">Configure Basic Settings for a Custom Poller Collection</a> for more information.</p> <p><b>Critical Status Conclusions</b></p> <table border="1"> <thead> <tr> <th>Conclusion</th> <th>Description</th> <th>Status</th> <th>Incident?</th> </tr> </thead> <tbody> <tr> <td>CustomPolledInstanceCritical</td> <td>A Custom Polled Instance is in a Critical State.</td> <td>Critical</td> <td>Y</td> </tr> </tbody> </table> <p><b>Major Status Conclusions</b></p>	Conclusion	Description	Status	Incident?	CustomPolledInstanceCritical	A Custom Polled Instance is in a Critical State.	Critical	Y
Conclusion	Description	Status	Incident?						
CustomPolledInstanceCritical	A Custom Polled Instance is in a Critical State.	Critical	Y						

Attribute	Description			
	<b>Conclusion</b>			
	<b>Description</b>	<b>Status</b>	<b>Incident?</b>	
	CustomPolledInstanceMajor	A Custom Polled Instance is in a Major State.	Major	Y
	<b>Minor Status Conclusions</b>			
	<b>Conclusion</b>			
	<b>Description</b>	<b>Status</b>	<b>Incident?</b>	
	CustomPolledInstanceMinor	A Custom Polled Instance is in a Minor State.	Minor	Y
	<b>Warning Status Conclusions</b>			
	<b>Conclusion</b>			
	<b>Description</b>	<b>Status</b>	<b>Incident?</b>	
	CustomPolledInstanceWarning	A Custom Polled Instance is in a Warning State.	Warning	Y
	<b>Normal Status Conclusions</b>			
	<b>Conclusion</b>			
	<b>Description</b>	<b>Status</b>	<b>Incident?</b>	
	CustomPolledInstanceNormal	A Custom Polled Instance is in a Normal State.	Normal	N

## Custom Polled Collection Form

The NNMi Custom Polling feature enables your NNMi administrator to take a proactive approach to network management by gathering additional device information using SNMP MIB Expressions. For example, an NNMi administrator might want NNMi to monitor the Status of COM (communication) ports on all of your Windows servers or determine disk utilization on a specified group of servers.

A Custom Poller Collection defines the additional SNMP MIB information that NNMi should gather (Custom Poll) as well as how NNMi reacts to the gathered data.

### For information about each tab:

**Note:** If the Security configuration permits, you can access a Comparison Map form from the Comparison Maps tab.

The following tables describe the attributes included on the Custom Polled Collection form.

### Basics for this Custom Poller Collection

Attribute	Description
Name	The name for the Custom Poller Collection configuration.  The Custom Poller Collection name appears in any incidents generated as a result of the collection.
Affect Node Status	Used to indicate whether each Polled Instance affects the associated Node's Status.  The first time a MIB Expression is validated with discovery information, the results appear in a Polled Instance object. The Polled Instance object is updated whenever a change in State occurs and includes the most recent polled value that caused the State to change.
Generate Incident	Used to indicate whether NNMi generates an incident: <ul style="list-style-type: none"> <li>when a threshold is crossed</li> <li>when a polled MIB value causes the Custom Polled Collection's State to be other than <b>Normal</b>.</li> </ul>
Export Custom Poller Collection	If enabled <input checked="" type="checkbox"/> , NNMi exports the Custom Poller Collection to a comma-separated values (CSV) file  If disabled <input type="checkbox"/> , NNMi does not export the Custom Poller Collection information.
Compress Export File	If enabled <input checked="" type="checkbox"/> , NNMi exports the Custom Poller Collection in compressed format and appends .gz to the .csv file suffix.  If disabled <input type="checkbox"/> , NNMi does not compress the CSV file.

### Variable Attributes

Attribute	Description
MIB Expression	MIB Expressions specify what additional information NNMi should gather.
MIB Filter Variable	The MIB Filter Variable is the MIB variable that has a value you want to use as a filter to determine which instances of the MIB expression to Custom Poll.

### High Threshold Attributes for a Custom Polled Instance

Monitored Attribute	Description
Threshold Setting Type	One of the following: <ul style="list-style-type: none"> <li><b>Count</b> threshold based on the number of occurrences specified before the threshold is reached.</li> <li><b>Time</b> threshold based on the duration of time specified before the threshold is reached.</li> </ul>



### High Threshold Attributes for a Custom Polled Instance, continued

Monitored Attribute	Description
High State	Possible values are: <ul style="list-style-type: none"> <li>• Normal</li> <li>• Warning</li> <li>• Minor</li> <li>• Major</li> <li>• Critical</li> </ul>
High Value	Designate the value that above which becomes a threshold situation. For special situations, the following values can be used: <ul style="list-style-type: none"> <li>• 0.0000000000000001 (or 1E-15 in Scientific Notation) for the smallest value greater than zero.</li> <li>• 99.99999999999999 for the highest value less than one hundred.</li> </ul> <p><b>Note:</b> If the maximum possible value, the High threshold is disabled because it cannot be <i>crossed</i>.</p>
High Value Rearth	The High Value Rearth designates the lower boundary of the High Threshold <i>range of values</i> .
<b>Threshold Setting Type = Count:</b>	
High Trigger Count	The number of consecutive polling intervals the returned value must be greater than the specified High Value to meet the High Threshold criteria.
<b>Threshold Setting Type = Time</b> (setting both of these to zero disables the High Threshold):	
High Duration	The minimum time within which the value must remain in the High range before the threshold state changes to High and (optionally) an incident is generated.
High Duration Window	The window of time within which the High Duration criteria must be met.

### Low Threshold Attributes for a Custom Polled Instance

Monitored Attribute	Description
Low State	Possible values are: <ul style="list-style-type: none"> <li>• Normal</li> <li>• Warning</li> <li>• Minor</li> </ul>

### Low Threshold Attributes for a Custom Polled Instance, continued

Monitored Attribute	Description
	<ul style="list-style-type: none"> <li>Major</li> <li>Critical</li> </ul>
Low Value	The value that <i>below which</i> indicates entering the Low range.  <b>Note:</b> If you use the minimum possible value, the threshold is disabled because it cannot be <i>crossed</i> .
Low Value Rearm	The Low Value Rearm designates the upper boundary of the Low Threshold <i>range of values</i> .
<b>Threshold Setting Type = Count:</b>	
Low Trigger Count	The number of consecutive polling interval the returned value must be less than the specified Low Value to meet the Low Threshold criteria.
<b>Threshold Setting Type = Time (setting both of these to zero disables the Low Threshold):</b>	
Low Duration	The minimum time within which the value must remain in the Low range before the threshold state changes to Low and (optionally) an incident is generated.
Low Duration Window	The window of time within which the Low Duration criteria must be met.

## Comparison Map Form

Custom Poller enables the NNMi administrator to map the returned value of a MIB Expression to a Custom Poller Polled Instance State. NNMi uses Comparison Map values to determine when to generate an incident, as well as the State of the Polled Instance.

[Click here for more information about Polled Instances.](#)

The first time a MIB Expression is validated with discovery information, the results appear in a Polled Instance object. The Polled Instance object is updated whenever a change in State occurs and includes the most recent polled value that caused the State to change.






For example, the NNMi administrator might configure a Custom Polled Collection so that the hrDeviceStatus value of **5** (down) is mapped to a **Critical** State. This means that NNMi changes the State of the Polled Collection Instance to **Critical** each time the hrDeviceStatus returns a value of **5** when polled.

The following tables describe the attributes included on the Comparison Map form.

### State Mapping Attributes

Attribute	Description
Ordering	The order in which the State mapping (Comparison Maps) operations should be performed.

**State Mapping Attributes, continued**

Attribute	Description
	<p><b>Note:</b> NNMi uses the Ordering value to determine which State mapping to use. The lower the number, the higher the priority. For example, 1 is the highest priority.</p>
Comparison Operator	<p>Operator used to evaluate the polled value and subsequently determine its State. For example, the &lt; (less than) Comparison Operator indicates the polled value returned must be less than the Comparison Value to change the Custom Poller Polled Instance to the state specified using the State Mapping value.</p>
Comparison Value	<p>The value to which the polled value is compared.</p>
State Mapping	<p>The State to assign to the Custom Poller Polled Instance when the polled value meets the comparison criteria. For example, each time the value <b>3</b> (warning) is returned when NNMi polls hrDeviceStatus, you can specify that you want NNMi to change the State of the Polled Instance to <b>Warning</b>.</p> <p>Possible State values for a <i>Polled Instance</i> (Threshold = High State/Low State; or Comparison Map = State Mapping) are:</p> <ul style="list-style-type: none"> <li> Normal</li> <li> Warning</li> <li> Minor</li> <li> Major</li> <li> Critical</li> </ul>

# Chapter 6

---

## 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 the next page

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

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:



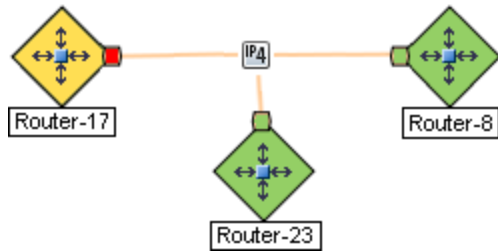
See [About Status Colors](#) for more information.

---

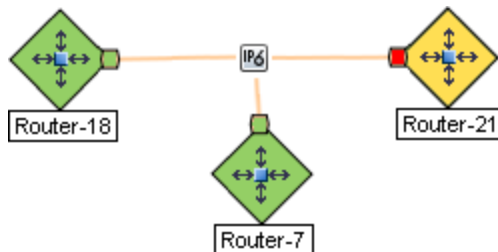
<sup>1</sup>Refers to the Data Link layer of the multilayered communication model, Open Systems Interconnection (OSI). The Data Link layer moves data across the physical links in the network. The switches and switch-routers are devices that redirect data messages at the layer 2 level, using the destination 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.

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:



*NNMi Advanced.* IPv6 subnets are indicated by this symbol:



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.

## 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 permits, you can configure the settings for a Node Group map, including selecting the background image. If the Node Group Map appears in a new window, use the **File** → **Open Node Group Map Settings** option. Administrators can also use the **User Interface Configuration** option from the Configuration workspace. See "Help for Administrators" for more information.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

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


**To access a Node Group map:**

- Display a map of all Node Groups and open a specific Node Group Map.
  - a. From the **Workspaces** navigation panel, select the **Topology Maps** workspace.
  - b. Select **Node Group Overview**.



- c. In the **Node Group Overview** map, double-click a  Node Group symbol.
- If you know the name of the Node Group that has the map you want to display, use the Troubleshooting workspace to open a map.
  - a. From the **Workspaces** navigation panel, select the **Troubleshooting** workspace.
  - b. Select **Node Group Map**.
  - c. In the **Node Group** field, enter the name of the Node Group that has the map you want to display.

**Note:** As you start typing the first few letters (case-sensitive) of the name of the node group, you will view a list that includes all potential node groups with names that match the letters or numbers as you enter them.
- Select from a table view of all Node Groups and open the map.
  - a. From the **Workspaces** navigation panel, select **Monitoring** or **Inventory** .
  - b. Select the **Node Groups** view.
  - c. In the Node Group view, select the row representing the Node Group of interest.
  - d. Select **Actions** → **Maps** → **Node Group Map**.
- Select any Node, Interface, or IP Address object and open the associated Node Group Map:
  - a. From the **Workspaces** navigation panel, select **Monitoring** or **Inventory** .
  - b. Select the Nodes, Interfaces, or IP Addresses view.
  - c. Select the row representing the object of interest.
  - d. Select **Actions** → **Maps** → **Node Group Map**.
- Select an Incident and open the Source Node's associated Node Group Map:
  - a. From the **Workspaces** navigation panel, select **Incident Management** or **Incident Browsing** .
  - b. Select any view.
  - c. Select the row representing the Incident of interest.
  - d. Select **Actions** → **Maps** → **Node Group Map**.

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

- You can view only the Node Groups that contain one or more nodes to which you have access.
- By default, each *Child* Node Group is represented by a  Node Group symbol that appears with the other Node objects in the *Parent* Node Group Map.

An NNMI administrator 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 \(NNMI Administrators only\)](#)" on page 229 for more information.

- **Child**  Node Group symbols can be moved and the new location saved with other Node objects in the map.
- To display the nodes within a *Child* Node Group, do one of the following:
  - Double-click the Node Group symbol.
  - Select the Node Group symbol and click the  **Open Node Group Map** icon.
  - Select the Node Group symbol and select **Actions** → **(Child Node Group Name) Map**.
- NNMi can enlarge the map symbol of any node associated with a **Key Incident**<sup>1</sup>. Use the **Indicate Key Incidents** button in the map view toolbar (see [Using the View Toolbars: Node Group Map Toolbar Icons](#)):



(on) = When the this Node Group map opens, NNMi enlarges any objects on a Node Group map that are Source Objects for a **Key Incident**<sup>2</sup>. (For example, when viewing the Node Group map, NNMi enlarges any node on a Node Group map that has an open root cause incident associated with it.)



(off) = When the this Node Group map opens, NNMi does not indicate the objects on a Node Group map that are Source Objects for a **Key Incident**<sup>3</sup>.

To view the associated incident for the node, double-click the node symbol. In the Node form, select the Incidents tab.

- *HP Network Node Manager iSPI Performance for Metrics Software only*. NNMi automatically synchronizes Interface Group and Node Group configuration changes between NNMi and NNM iSPI Performance for Metrics. However, in some cases, additional configuration changes that affect Node Group or Interface Group membership might take longer to synchronize.

If you do not see one or more nodes in an NNMi Performance for Metrics report that are visible in NNMi, use the **Actions** → **NNM iSPI Performance** → **Synch Report Groups** with NNMi option. This option forces NNMi to synchronize the Interface and Node Group information between NNMi and NNM iSPI Performance for Metrics more quickly than the default time frame.

NNMi provides the "[Node Group Overview Map](#)" on page 257. Your NNMi administrator can provide more Node Group maps.

#### Related Topics

["Navigating within a Node Group Map" on the next page](#)

["Position Nodes on a Node Group Map" on page 257](#)

---

<sup>1</sup>Incidents with both: (1) Severity = other than Normal. (2) Correlation Nature = equal to Root Cause, Service Impact, Stream Correlation, Rate Stream Correlation, Info, or None.

<sup>2</sup>Incidents with both: (1) Severity = other than Normal. (2) Correlation Nature = equal to Root Cause, Service Impact, Stream Correlation, Rate Stream Correlation, Info, or None.

<sup>3</sup>Incidents with both: (1) Severity = other than Normal. (2) Correlation Nature = equal to Root Cause, Service Impact, Stream Correlation, Rate Stream Correlation, Info, or None.


## 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, double-click the Child Node Group object:



**Tip:** Select the  node group object and click  Open to display the Child Node Group form.

- To return to a previous Node Group Map, use the breadcrumbs in the map's title bar.
- To display a Node Group Map for a Child Node Group in a new window, do one of the following:
  - Use **Actions** → **Maps** → **Node Group Map**.
  - Click  Show Map in New Window.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

**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 open the Node Group form for the displayed Node Group map, do one of the following:  
Select **File** → **Open Node Group for Map**.
- To open the Node Group Map Settings form from the displayed Node Group map, select **File** → **Open Node Group Map Settings**.
- You can manually reposition the nodes on the background image, and, if your role permits, save the map for later use. See "[Position Nodes on a Node Group Map](#)" on the next page for more information.
- NNMi can enlarge the map symbol of any node associated with a [Key Incident](#)<sup>1</sup>. Use the **Indicate Key Incidents** button in the map view toolbar (see [Using the View Toolbars: Node Group Map Toolbar Icons](#)):



(on) = When the this Node Group map opens, NNMi enlarges any objects on a Node Group map that are Source Objects for a [Key Incident](#)<sup>2</sup>. (For example, when viewing the Node Group map, NNMi enlarges any node on a Node Group map that has an open root cause incident associated with it.)

---

<sup>1</sup>Incidents with both: (1) Severity = other than Normal. (2) Correlation Nature = equal to Root Cause, Service Impact, Stream Correlation, Rate Stream Correlation, Info, or None.

<sup>2</sup>Incidents with both: (1) Severity = other than Normal. (2) Correlation Nature = equal to Root Cause, Service Impact, Stream Correlation, Rate Stream Correlation, Info, or None.





(off) = When the this Node Group map opens, NNMi does not indicate the objects on a Node Group map that are Source Objects for a **Key Incident**<sup>1</sup>.

To view the associated incident for the node, double-click the node symbol. In the Node form, select the Incidents tab.

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

## Position Nodes on a Node Group Map

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

**Note:** If your role permits, 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. Select the row that represents the Node Group of interest.
  - d. Select **Actions** → **Maps** → **Node Group Map**.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

2. Manually re-position the node locations by dragging and dropping the nodes to the location you want.
3. If your role permits, 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:

---

<sup>1</sup>Incidents with both: (1) Severity = other than Normal. (2) Correlation Nature = equal to Root Cause, Service Impact, Stream Correlation, Rate Stream Correlation, Info, or None.

- 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](#)

## Initial Discovery Progress or Network Overview Map

**Initial Discovery Progress** displays a map containing the most highly connected nodes (largest subnets) in the Layer 3 network. Use this map to display the initial discovery progress of the Routers, Switches, and Switch-Routers, for up to 100 nodes.

**Note:** NNMi displays this map only if the NNMi administrator has configured the NNMi console's Initial View to be **Installation Default** and the network has less than or equal to a total of 100 routers, switches, and switch-routers. After NNMi has discovered more than 100 connectors, this map view changes to the Open Key Incidents table view.

To determine which nodes to display, NNMi uses the following algorithm until it has displayed a maximum of 100 nodes:

- Display the largest subnets (Layer 3 connectivity) based on discovered routers
- Display the most highly connected switches within the subnets displayed
- Display the most highly connected nodes within the subnets displayed
- Display any remaining nodes up to a total of 100

Note the following:

- NNMi polls only management IP addresses by default. Therefore, the status of IP addresses on the map might appear as No Status (□).
- Because the connections on a Layer 3 represent subnets, which are not monitored in NNMi, the connections on a the Initial Discovery Progress map appear as No Status (—).
- The **Initial Discovery Progress** map displays a maximum of 100 nodes. This maximum number cannot be changed.

The **Initial Discovery Progress** 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

The **Network Overview** map is similar to the **Initial Discovery Progress** map with the following exceptions:

- Network Overview displays a map containing the most highly connected nodes (largest subnets) in the Layer 3 network for up to 250 nodes.
- The NNMi administrator can change the maximum number of nodes displayed. If you are an NNMi administrator, see "NNMi Console" in the HP Network Node Manager i Software Deployment Reference for more information.
- The refresh rate is 5 minutes.
- The NNMi administrator must have configured the NNMi console's Initial View to be **Network Overview**

**To display the Initial Discovery Progress or Network Overview map using the Topology Maps workspace:**

1. From the workspace navigation panel, select the **Topology Maps** workspace.
2. Select **Initial Discovery Progress** or **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 44 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 switch-routers. (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 attribute value from the "[Node Form](#)" on page 50 or any IP Address belonging to a node in your network. (NNMi provides a case-sensitive drop-down list to help speed up your selection.)

---

<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 switch-routers 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.

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.

The color of the line between the devices indicates the health of the connection ( See "[Viewing Maps \(Network Connectivity\)](#)" on page 252).

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** workspace, **Nodes** view.

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

For example, select the row representing 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.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

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 252).

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 188 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 188](#)

## 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 Neighbor View maps are nodes that have a Device Category value of either router or switch-router. (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.

---

<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.

- 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 attribute value from the "[Node Form](#)" on page 50 or any IP Address belonging to a node in your network. (NNMi provides a case-sensitive drop-down list to help speed up your selection.)

**Note:** You can enter a **Node or IP** attribute value that represents a node of any Device Category. On the Layer 3 Neighbor View map, NNMi displays only those devices that have a Device Category of **router** or **switch-router** that are connected to it.

4. A hop represents a network device that has a Device Category value of either **router** or **switch-router** and 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 252).

**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** workspace, **Nodes** view.

2. Select the initial object of interest.

For example, select the row that represents the node of interest from the **Nodes** view.

3. Select **Actions** → **Layer 3 Neighbor View**.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

4. A hop represents a network device that has a Device Category value of either router or switch-router and 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 connection (see "[Viewing Maps \(Network Connectivity\)](#)" on page 252).



**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 154 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](#)

## 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 272.

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. 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 or routers.

To view all possible connections between nodes, use the Layer 2 Neighbor View. See "[Display the Layer 2 Neighbor View](#)" on page 261 for more information.

**Note:** End nodes are the primary use case for this view. If you specify 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 267). 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 281 for more information about Router Redundancy Groups. See "[Path Calculation Rules](#)" on page 267 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 272 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.

*HP Network Node Manager iSPI Performance for Metrics Software.* You can view a report of the Path Health from the Path View map using the **Actions** → **HP NNM iSPI Performance** → **Reporting - Path Health** menu. Before using the menu option, you must select the starting and ending node for which you want to view the health information. The nodes you select must reside in the NNMi topology database and be configured for performance measurement collection. See the NNM iSPI Performance for Metrics online help for more information.

*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 272 for more information.



*NNMi Advanced.* Path View works only with IPv4 addresses. The NNMi Advanced IPv6 address values are not valid choices for Path View. Any devices in your network that are configured with IPv6 addresses cannot be displayed on Path View maps.

**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 Tool Tips information about that object.

**Note:** You see only those nodes in the Path View that you have permission to view. NNMi ignores any nodes to which you do not have access and generates the path as if these nodes were not discovered. If you are an NNMi administrator, see [Configuring Security](#) for more information about configuring security, including node access.

See [Path View Map Objects](#) for more information about the symbols that might appear on a Path View map. See [About Status Colors](#) for information about possible Status colors.

**Tip:** Click the  Swap Nodes icon to switch the **Source** and **Destination** values, and then click the  Compute Path icon. 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**.

**Note:** You can designate any node as Source / Destination, the node does not need to currently be included in the NNMi database.

3. In the **Source** field, type a valid fully-qualified hostname, short hostname, or IPv4 address. (If your entry matches an object currently in the NNMi database, NNMi provides a case-sensitive drop-down list to help speed up your selection.)
4. *Optional.* In the **Destination** field, type a valid fully-qualified hostname, short hostname, or IPv4 address.

If a **Destination** value is not provided, NNMi displays the path from the **Source** node to its access router. (If your entry matches an object currently in the NNMi database, NNMi provides a case-sensitive drop-down list to help speed up your selection.)

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**). Select the row representing that object.
3. *Optional.* Decide which object you want to use as the destination point in the path (**Destination**). Select 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** → **Maps** → **Path View**.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

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

**Related Topics:**

["Path Calculation Rules" below](#)

["Investigate Errors and Performance Issues" on page 271](#)

["Access Node Details" on page 287](#)

## Path Calculation Rules

**Note:** If NNMi Advanced is licensed and installed, also see ["Enhanced Path View \(NNMi Advanced\)" on page 272](#)

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*) Path View works only with IPv4 addresses. The NNMi Advanced IPv6 address values are not valid choices for Path View. Any devices in your network that are configured with IPv6 addresses cannot be displayed on Path View maps.

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



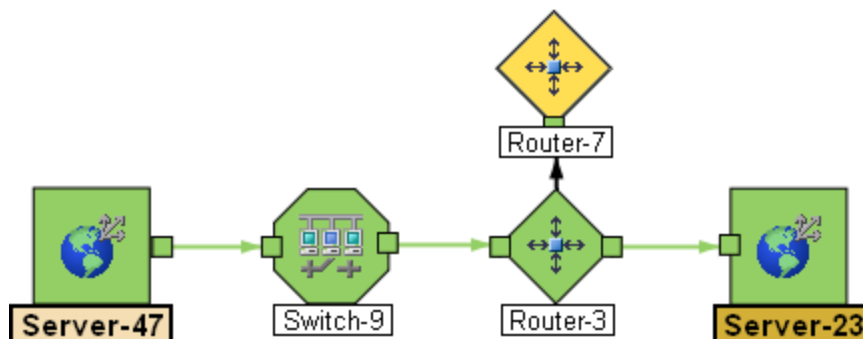
- If a missing connection is detected (no response to SNMP and no entry in `PathConnections.xml`), the cloud symbol appears in the routing core between the access routers.
- If the port connecting the end node to the first switch is forwarding more than one MAC address, this indicates an intermediate 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:

- In Path View maps, a black arrow or empty black circle that appears at the end of a connection indicates that NNMi was not able to determine a status value because the connection or interface is not in the NNMi database. Reasons a connection or interface are not stored in the NNMi database, include the following:
  - NNMi is unable to collect information about a node in the path because it is a non-SNMP node.
  - Not all of the nodes in the path are managed by NNMi.
  - The discovery information for a node is not up-to-date (for example, interface information is missing).
- You see only those nodes in the Path View that you have permission to view. NNMi ignores any nodes to which you do not have access and generates the path as if these nodes were not

discovered. If you are an NNMi administrator, see [Configuring Security](#) for more information about configuring security, including node access.

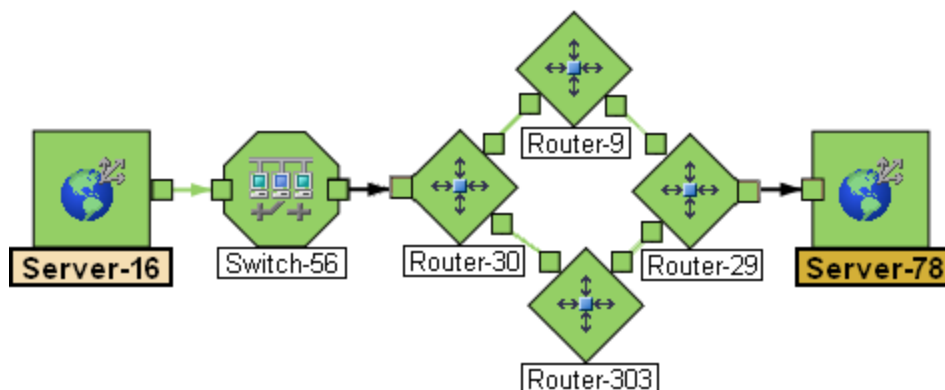
- The Source and Destination nodes must meet *either* of the following criteria:
  - Support SNMP and be previously discovered by NNMi (recorded in the topology database)
  - Have traceroute available
- A switch should not be used as a Source or Destination node in Path View maps. To view connectivity between switches, use the Layer 2 Neighbor View.
- 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 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:



- (*NNMi Advanced*) If your network administrator configures NNMi to gather data from Route Analytics Management Systems (RAMS), the Path View can show multiple **OSPF**<sup>1</sup> Equal Cost paths through a Layer 3 cloud as shown in the example below:

---

<sup>1</sup>Open Shortest Path First Protocol



**Note:** When RAMS data is used to determine the router paths, NNMi ignores the `PathConnections.xml` file. See "Enhanced Path View (NNMi Advanced)" on page 272 for more information.

- (HP Network Node Manager iSPI Performance for Metrics Software) You can access performance data from Path Views that contain single or multiple paths. See "Investigate Errors and Performance Issues" on the next page" for more information

#### Related Topics:

[Use Map Views](#)

"Path View Limitations" below

## 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.

**Note:** *NNMi Advanced*. Path View works only with IPv4 addresses. The NNMi Advanced IPv6 address values are not valid choices for Path View. Any devices in your network that are configured with IPv6 addresses cannot be displayed on Path View maps.

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 272 for more information.

**Caution:** Do not specify a switch as a Source or Destination node in Path View maps. To view connectivity between switches, use the Layer 2 Neighbor View.

- 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.
- If the NNMI administrator enabled **MPLS**<sup>1</sup>, Path view can show multiple OSPF Equal Cost paths.

## 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 285 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 287
- "[Access a Problem Device](#)" on page 287
- "[Access All Related Incidents](#)" on page 290

See "[Interpret Root Cause Incidents](#)" on page 387 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 > HP NNM iSPI Performance > 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 > HP NNM iSPI Performance > Reporting - Path Health**.

**Note:** *NNMi Advanced*. Path View works only with IPv4 addresses. The NNMI Advanced IPv6 address values are not valid choices for Path View. Any devices in your network that are configured with IPv6 addresses cannot be displayed on Path View maps.

## MPLS WAN Cloud Map (*NNMi Advanced*)

The MPLS WAN Cloud Map view displays a graphical representation the Layer 3 connectivity in your network, as well as any Customer Edge and Provider Edge devices. This map periodically updates the Customer Edge (CE) status. The MPLS WAN discovery updates the topology, (see [To discover MPLS WANs in the network](#)). The update interval is more frequent when the topology is changing and less frequent when the topology is not changing.

**To discover MPLS WAN's in the Network:**

---

<sup>1</sup>Multiprotocol Label Switching

After integrating with RAMS IM, NNMi startup discovers all the MPLS WAN's in the network.

1. From the workspace navigation panel, select the **Inventory** workspace.
2. Select the **MPLS WAN Clouds (RAMS)**.
3. From the **Actions** menu, select **Discover MPLS WANs**.  
This discovers all the MPLS WAN's in the network.





**To display the MPLS WAN Cloud Map view:**

1. In the MPLS WANs Cloud table view, select a row.
2. From the **Actions** menu, select **MPLS WAN Cloud View**.  
This displays the selected object's Cloud view.

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

- View a high-level overview of your MPLS WAN Cloud
- Determine the most highly connected nodes in the Layer 3 network

The symbols used in MPLS WAN Cloud view are described in the following table:

Symbol	Description
	The MPLS WAN Cloud. The icon indicates that the status of the devices in the cloud is unknown.
	The IP address of the Provider Edge (PE) device. Status of a PE is indicated by the color. For example, blue color indicates that the status of the device is unknown. For more information, see <a href="#">Status Color and Meaning for Objects</a> .
	The CE router that is participating in the MPLS WAN cloud.
	The Interface on the CE router that is peering with the PE device. The color of the icon shows the status of the CE router. For more information, see <a href="#">Status Color and Meaning for Objects</a> .

**Tip:** Select the connector between PE device and CE router to view the IP addresses of the PE device and the Interface name of CE router.

**Related Topics**

"MPLS WAN Cloud (RAMS) Form (NNMi Advanced)" on page 235

"MPLS WAN Cloud (RAMS) Form: MPLS WAN Connections Tab (NNMi Advanced)" on page 236

## Enhanced Path View (NNMi Advanced)

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



- Router Redundancy Protocol group members (for example, [HSRP](#)<sup>1</sup> or [VRRP](#)<sup>2</sup>)

By default, NNMi monitors [current state](#) and priority information for any discovered Router Redundancy Group objects in the network. If the configured Router Redundancy Protocol allows virtual addresses, NNMi includes those virtual addresses when calculating the Path View.

- HP Router Analytics Management System ([RAMS](#)<sup>3</sup>) data

If your NNMi Administrator established any RAMS server configurations, 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.)

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

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. More than one path appears if HP Router Analytics Management System (RAMS) determines more than one equal cost path and, therefore, cannot determine which path is in use.

**Note:** *NNMi Advanced*. Path View works only with IPv4 addresses. The NNMi Advanced IPv6 address values are not valid choices for Path View. Any devices in your network that are configured with IPv6 addresses cannot be displayed in Path View maps.

---

<sup>1</sup>Hot Standby Router Protocol

<sup>2</sup>Virtual Router Redundancy Protocol

<sup>3</sup>HP Router Analytics Management System

# Chapter 7

---

## 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 status other than normal, 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 26](#)

["Monitor with Table Views" below](#)

["Monitor with Map Views" on page 284](#)

["Monitor with Line Graphs" on page 294](#)

## 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:

Note the following:

- NNMi uses Conclusions to determine an object's Status. Therefore, an object with a non-Normal Status does not always have an open incident associated with it. See [The NMMi Causal Engine and Object Status](#) for more information about incidents, conclusions, and object Status.
- If NNMi determines that it requires more time to complete its analysis for an object, one of the following occurs:
  - There is a delay between the change in object Status and any associated open incident.
  - NNMi determines that the incident does not apply and the incident is not generated.

For example, when an address is not responding to ICMP, the Status of the address is set to Critical, but the incident is delayed until the NNMi Causal Engine determines whether the address is in the shadow of a node that is down. If the address is in the shadow of node that is down, NNMi does not generate an Address Not Responding incident. If the address is not in the shadow of a node that is down, NNMi generates the Address Not Responding incident. See [Node Down](#) for more information about objects that are in the shadow of a node.

- If Dampening is configured for the incident, one of the following occurs:
  - There is a delay between the change in object Status and any associated open incident.  
**Tip:** To see an incident that has a Lifecycle State of **Dampened**, in the NNMi console, select either the **Custom Incidents** or **Open Custom Incidents** view and set the **Lifecycle State** Filter to **Dampened**.
  - NNMi determines that the incident does not apply and the incident is automatically deleted.  
If you are an NNMi administrator, see [Dampening Incident Configurations](#) for more information.
- If the Incident Configuration is suppressed, NNMi does not display the incident. If you are an NNMi administrator, see [Suppress Incident Configurations](#) for more information.

**Tip:** To view the nodes that have an open associated incident from a Node Group Topology Map view, click  **Indicate Key Incidents**. This option enlarges each object on the map that has an associated open incident. This option is available only with Node Group maps.

["Non-Normal Node Components View"](#) below

["Non-Normal Cards View"](#) on the next page

["Non-Normal Interfaces View"](#) on the next page

["Non-Normal Nodes View"](#) on page 277

["Non-Normal SNMP Agents View"](#) on page 279

["Not Responding Address View"](#) on page 279

["Interface Performance View \(NNM iSPI Performance for Metrics\)"](#) on page 280

["Card Redundancy Groups View \(Monitoring\)"](#) on page 280

["Node Groups View \(Monitoring\)"](#) on page 282

["Custom Node Collections View \(Monitoring\)"](#) on page 282

["Custom Polled Instances View"](#) on page 282

## Non-Normal Node Components View

The Non-Normal Node Components view in the Monitoring workspace is useful for identifying all of the Node Components that might need operator attention. Examples of Node Components include temperature, fan, and memory.

Possible Statuses for these interfaces include:

- Warning
- Major
- Minor
- Critical

**To display the Non-Normal Node Component view:**

1. In the **Workspaces** navigation pane, select the **Monitoring** workspace.
2. Select the **Non-Normal Node Component** view.

For each Node Component displayed, you can see its Status, Name, Type, the Node in which it resides, and the date and time the Status was last modified.

### **Related Topics**

[Use Table Views](#)

[Export Table Information](#)

## **Non-Normal Cards View**

**Tip:** See "Card Form" on page 157 for more details about the attributes that appear in this view's column headings.

The Non-Normal Cards view in the Monitoring workspace is useful for identifying all of the Cards that have a status that is other than Normal.

### **To display the Critical Cards view:**

1. In the **Workspaces** navigation pane, select the **Monitoring** workspace.
2. Select the **Critical Cards** view.

For each Card displayed, you can see its Administrative State, Operational State, the Node on which it resides (Hosted on Node), the date and time the Status was last modified, the Card Name, Model, Type, Serial Number, Firmware Version, Hardware Version, Software Version, Index number, Physical Index number, the Card on which it is hosted, if any, the Card Redundancy Group of which it is a member, if any, the date and time the State was last modified, the Card description, and any notes for the Card.

### **To see the incidents related to a Card:**

1. Double-click the row representing the Card that has the incidents you want to see.
2. Navigate to the **Incidents** tab to see the incidents associated with the selected Card.

### **Related Topics**

[Use Table Views](#)

[Export Table Information](#)


## **Non-Normal Interfaces View**

**Tip:** See "Interface Form" on page 90 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 `AdministrativeState` equal to  **Up**.

**To display the Non-Normal Interfaces view:**

1. In the **Workspaces** navigation pane, select the **Monitoring** workspace.
2. Select the **Non-Normal Interfaces** view.

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.
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.  <b>Tip:</b> You can right-click any object in a table or map view to access the <b>Actions</b> menu.

### Related Topics

[Use Table Views](#)

[Export Table Information](#)

## Non-Normal Nodes View

**Tip:** See "[Node Form](#)" on page 50 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 operator 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, whether the SNMP Agent is enabled on the node, 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.
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 50</a> and <a href="#">"IP Subnet Form" on page 154</a> for more information.
Access a map view of a selected node and its surrounding topology	<p>Select the node of interest and use the Actions menu from the main toolbar. See <a href="#">Use Table Views</a> for more information.</p> <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;"> <p><b>Tip:</b> You can right-click any object in a table or map view to access the <b>Actions</b> menu.</p> </div>
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 SNMP Agents View

**Tip:** See "SNMP Agent Form" on page 140 for more details about the SNMP Agent attributes that appear in this view's column headings.

The **Non-Normal SNMP Agents** view in the **Monitoring** workspace is useful for identifying all of the SNMP Agents that have a state that is other than Normal.

### To display the Non-Normal Node SNMP Agents view:

1. In the **Workspaces** navigation pane, select the **Monitoring** workspace.
2. Select the **Non-Normal SNMP Agents** view.

For each SNMP Agent displayed in the view, you can identify the SNMP Agent Status, the Agent SNMP State, the Agent ICMP State, the associated node Name value (**Hosted On Node**), the IP address NNMi uses to communicate with this SNMP agent (Management Address), the date and time the Status was last modified, the version of the SNMP protocol in use, whether the SNMP agent is set up for SNMP communication in the network environment (Agent Enabled), the User Datagram Protocol port configuration for this SNMP agent (UDP Port), the time that NNMi waits for a response to an SNMP query before reissuing the request, and the maximum number of retries that NNMi issues for an SNMP query before determining the query result to be "unresponsive", the read community string, and the SNMP Proxy address.

**Note:** If you have Administrator Role, the Non-Normal SNMP Agents view also displays the Read Community String.

### Related Topics

[Use Table Views](#)

[Print Table Information](#)

## Not Responding Address View

**Tip:** See "IP Address Form" on page 132 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 that has a state that is  **Not Responding** (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**), the date and time the State was last modified, the prefix length (**PL**), and any notes included for the IP address.

### Related Topics

[Use Table Views](#)

[Export Table Information](#)

## Interface Performance View (*NNM iSPI Performance for Metrics*)

(*NNM iSPI Performance for Metrics*) Data appears in this view only if the HP Network Node Manager iSPI Performance for Metrics Software is installed and your NNMi administrator enables performance monitoring.

The interface performance view helps you identify the over-used and under-used interfaces within nodes in your network. Sort this view by Hosted On Node to help identify which nodes receive the most traffic. You can proactively monitor your network and check for those interfaces that have an input or output utilization, error, or discard rate that indicates there might be a potential problem.

Your network administrator can set up Node Groups or Interface Groups that identify important network devices, and those groups can be filters for this view.

**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 polling states for its input and output utilization rates, input and output utilization baselines, input and output error rates, input and output discard rates, Frame Check Sequence (FCS) error rates, input and output queue drops, 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 90 for more details about the interface attributes that appear in this view's column headings.

## Card Redundancy Groups View (Monitoring)

**Tip:** See "[Card Redundancy Group Form](#)" on page 204 for more details about the Card Redundancy Group attributes that appear in this view's column headings.

Your network administrator might have set up groups of redundant cards to provide one-to-one redundancy protection against processor card failure.

### To display the Card Redundancy Groups view:

1. In the **Workspaces** navigation pane, select the **Monitoring** workspace.
2. Select the **Card Redundancy Groups View** view.

For each Card Redundancy Group displayed in the view, you can identify the Card Redundancy Group Status, Name, and the time and date the Card Redundancy Group Status was last modified.

### To see the incidents related to a Card Redundancy Group:

1. Double-click the row representing the Card Redundancy Group that has incidents you want to see.



2. Select the **Incidents** tab.

A table displays the list of Incidents associated with the selected Card Redundancy Group.

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

1. Double-click the row representing the Card Redundancy Group that has members you want to see.
2. Select the **Redundant Cards** tab.

A table displays the list of Cards that belong to the selected Card Redundancy Group.

## Router Redundancy Group View (NNMi Advanced)

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.

**Tip:** See "[Router Redundancy Group Form \(NNMi Advanced\)](#)" on page 209 for more details about the Router Redundancy Group attributes that appear in this view's column headings.

**To display the Router Redundancy Group view:**

1. In the **Workspaces** navigation pane, select the **Inventory** workspace or the **Monitoring** workspace.
2. Select the **Router Redundancy Group** view.

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. Double-click the row representing a Router Redundancy Group. The "[Router Redundancy Group Form \(NNMi Advanced\)](#)" on page 209 displays all details about the selected Router Redundancy Group.
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:**

1. Double-click the row representing the Router Redundancy Group members you want to see.
2. Navigate to the **Router Redundancy Members** tab.

Each node that belongs to the selected Router Redundancy Group is listed. You also see which interface is assigned to the Router Redundancy Group within each node.

### Related Topics

[Use Table Views](#)

[Export Table Information](#)

## Node Groups View (Monitoring)

**Tip:** See "Node Group Form" on page 223 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 can 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 Views by Node or Interface Group" on page 26 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 software, and any notes about the node group.

## Custom Node Collections View (Monitoring)

**Tip:** Mouse over a column heading for the complete name of a column heading attribute. See "Custom Node Collections Form" on page 237 for more details about the attributes that appear in the view's column headings.

The **Custom Node Collections** view in the **Monitoring** workspace is useful for identifying the node objects for which Custom Poller Polices have been created.

For each Custom Node Collection displayed, you can identify a Custom Node Collection's overall [Status](#), the Name of the associated topology node, the [Active State](#) of the Custom Node Collection's Policy, the name of the Policy that is applied to the current Custom Node Collection, as well as discovery information regarding the MIB Expression on each node for which you are collecting data, such as [Discovery State](#), the Discovery State Last Modified, and Discovery State Information.

### Note the following:

- The Custom Node Collection's Status is the most severe State value returned from the Polled Instances for the Custom Node Collection.
- The Active State for any Custom Node Collection associated with a Not Managed or Out of Service node that was previously managed, becomes **Inactive**. NNMi deletes all of the Polled Instances associated with the Not Managed or Out of Service node.
- You can display a Line Graph for those incidents that have a source node associated with Custom Node Collections. See "Display a Line Graph from an Incident (Custom Poller Only)" on page 306 for more information.

## Custom Polled Instances View

**Tip:** Mouse over a column heading for the complete name of a column heading attribute. See "Custom Polled Instance Form" on page 242 for more details about the attributes that appear in

the view's column headings.

The Custom Polled Instances view in the **Monitoring** workspace is useful for viewing the polling results for **Custom Node Collection**<sup>1</sup>. A Custom Polled Instance represents the results of a MIB expression when it is evaluated against a node in the Custom Node Collection. The first time a MIB Expression is validated with discovery information, the results appear in a Custom Polled Instance object. The Custom Polled Instance is updated whenever a change in State occurs and includes the most recent polled value that caused the State to change. For more information, click here.

A node can be associated with multiple Custom Polled Instances when its associated MIB expression includes MIBs that have multiple instances per node. For example, the associated MIB expression might perform a calculation using the ifInOctets and ifOutOctets MIB values. Using the MIB Filter and MIB Filter Variable specified, NNMi calculates these values for each interface that meets the filter criteria and that is associated with a node in the Custom Poller Collection.

**Note:** The **Active State** for any Custom Node Collection associated with a Not Managed or Out of Service node that was previously managed, becomes **Inactive**. NNMi deletes all of the Polled Instances associated with the Not Managed or Out of Service node.

For each Custom Polled Instance displayed, you can identify the following:

- **Status** of the Custom Polled Instance
- **State** of the Custom Polled Instance
- Returned value from the MIB Expression that caused the State to change
- MIB Expression name
- MIB Instance value
- Filter Value (The instance of a MIB variable value after the MIB Filter is applied)
- The Display Attribute (The value that results from the Instance Display Configuration. The NNMi administrator can specify the Instance Display Configuration information when configuring a MIB expression for Custom Poller.)
- Name of the topology Node on which the Custom Poller Policy information is being collected
- Name of the associated **Custom Node Collection**<sup>2</sup>.
- **Active State**
- Date and time the Custom Polled Instance State was last modified

*(NNMi Advanced - Global Network Management feature)* Any Custom Polled Instances are not sent from a Regional Manager (NNMi management server) to the Global Manager. From the Global Manager, use **Actions** → **Open from Regional Manager** to see the list of Custom Polled Instances on the Regional Manager.

---

<sup>1</sup>A Custom Node Collection identifies a topology node that has at least one associated Custom Poller Policy. Because a topology node can be associated with more than one Policy, the same topology node might appear in multiple Custom Node Collections.

<sup>2</sup>A Custom Node Collection identifies a topology node that has at least one associated Custom Poller Policy. Because a topology node can be associated with more than one Policy, the same topology node might appear in multiple Custom Node Collections.

## Monitor with Map Views

NNMi provides four kinds of map views that show a graphical representation of a selected device and the devices connected to it (Node Group Map views, 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:** Some NNMi users can delete nodes and other objects from the NNMi database (depending on the assigned NNMi Role). Any node that has been deleted appears as a transparent icon to all NNMi users until their 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 **Initial Discovery Progress** and **Network Overview** maps.

To monitor your network using a network map:

- ["Watch Status Colors" on the next page](#)
- ["Determine Problem Scope" on page 286](#)
- ["Access Node Details" on page 287](#)

### Related Topics:

#### Use Map Views

["Node Group Maps" on page 253](#)

["Display the Layer 2 Neighbor View" on page 261](#)

["Display the Layer 3 Neighbor View" on page 263](#)

["Path Between Two Nodes that Have IPv4 Addresses" on page 265](#)

## Watch Status Colors

When monitoring the network using a map view, watch for nodes that have a Status color of non-Normal. The background shapes of the map symbols change color based on the current health status of the represented device.

Note the following:

- NNMi uses Conclusions to determine an object's Status. Therefore, an object with a non-Normal Status does not always have an open incident associated with it. See [The NMMi Causal Engine and Object Status](#) for more information about incidents, conclusions, and object Status.
- If NNMi determines that it requires more time to complete its analysis for an object, one of the following occurs:
  - There is a delay between the change in object Status and any associated open incident.
  - NNMi determines that the incident does not apply and the incident is not generated.


For example, when an address is not responding to ICMP, the Status of the address is set to Critical, but the incident is delayed until the NNMi Causal Engine determines whether the address is in the shadow of a node that is down. If the address is in the shadow of node that is down, NNMi does not generate an Address Not Responding incident. If the address is not in the shadow of a node that is down, NNMi generates the Address Not Responding incident. See [Node Down](#) for more information about objects that are in the shadow of a node.

- If Dampening is configured for the incident, one of the following occurs:
  - There is a delay between the change in object Status and any associated open incident.

**Tip:** To see an incident that has a Lifecycle State of **Dampened**, in the NNMi console, select either the **Custom Incidents** or **Open Custom Incidents** view and set the **Lifecycle State** Filter to **Dampened**.
  - NNMi determines that the incident does not apply and the incident is automatically deleted.


If you are an NNMi administrator, see [Dampening Incident Configurations](#) for more information.

- If the Incident Configuration is suppressed, NNMi does not display the incident. If you are an NNMi administrator, see [Suppress Incident Configurations](#) for more information.











**Tip:** To view the nodes that have an open associated incident from a Node Group Topology Map view, click  **Indicate Key Incidents**. This option enlarges each object on the map that has an associated open incident. This option is available only with Node Group maps.

The following table describes the meaning for each Status color that might appear on a map. The Status categories are listed in decreasing order of Severity.

### 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</li></ul>

### Status Colors, continued

Color	Meaning	Description
		<p>yet calculated.</p> <ul style="list-style-type: none"> <li>The node is unreachable and cannot be polled.</li> </ul>
	Disabled	Indicates the object is administratively "disabled". (For example: for an interface, the current value of the MIB-II ifAdminStatus is "disabled".)
	Critical	Indicates NNMi detected problems that require immediate attention.
	Major	Indicates NNMi detected problems that could precede a critical situation.
	Minor	Indicates NNMi has detected problems related to the associated object that require further investigation.
	Warning	Indicates there might be a problem related to the associated object.
	Normal	Indicates there are no known problems related to the associated object.
	No Status	<p>Indicates that NNMi monitoring configuration specifically excludes this device. The Status is either not calculated or the device is Not Managed/Out Of Service.</p> <p>In Path View maps, note the following:</p> <ul style="list-style-type: none"> <li>A black arrow or empty black circle that appears at the end of a connection indicates that NNMi was not able to determine a status value because the connection or interface is not in the NNMi database.</li> <li>Reasons a connection or interface are not stored in the NNMi database, include the following:           <ul style="list-style-type: none"> <li>NNMi is unable to collect information about a node in the path because it is a non-SNMP node.</li> <li>Not all of the nodes in the path are managed by NNMi</li> <li>The discovery information for a node is not up-to-date (for example, interface information is missing)</li> </ul> </li> </ul>
	Node Not Accessible	<p>Indicates a node that you cannot access according to your Security Group membership. For example in a Path View, NNMi might include information about all nodes in the path, whether you can access additional information about each node.</p> <p>This Status might also indicates that a node has been removed from the NNMi database since the last  Refresh of the data you are viewing.</p>

## 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 454.
- Use telnet to access the device and determine more information, see "[Establish Contact with a Node \(Telnet or Secure Shell\)](#)" on page 456.
- Use traceroute to view traffic paths, see "[Find the Route \(traceroute\)](#)" on page 455.

**Note:** Access to these commands depends on the [NNMI Role](#)<sup>1</sup> and Object Access Privileges to which you are assigned. If you are unable to access an action, contact your NNMI administrator.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.


## 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 an Analysis Pane that displays 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.


---

<sup>1</sup>Determined by your membership in one of four special NNMI User Groups (NNMI Administrators, NNMI Level 2 Operators, NNMI Level 1 Operators, or NNMI Guest Users). This membership determines what you can see and do within the NNMI console.

**To access the Analysis Pane from a table view:**

1. Select the workspace of interest (for example,  **Inventory**).
2. Select the view that contains the object of interest (for example, the **Nodes** view).
3. Select the row that contains the object of interest.
4. NNMi displays detailed information at the bottom of the view in the Analysis Pane.


**To access the Analysis Pane in a map view:**


1. Select the workspace of interest (for example,  **Topology Maps**).
2. Select a map view (for example, select **Routers**).

**Note:** If the map requires a starting node before it opens, enter the name or IP Address for the starting node you want to use.

3. Click the map object of interest.
4. NNMi displays detailed information at the bottom of the view in the Analysis Pane.

**To access the Analysis Pane in a form:**

- Click the form's toolbar  Show Analysis icon to display information about the current form's top-level object in the Analysis Pane.

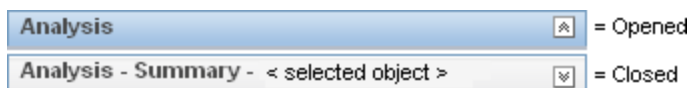
**Note:**  Show Analysis always displays the top-level object's information.

- Click a row in a table on one of the form's tabs to display detailed information about the selected object in the Analysis Pane.



NNMi displays detailed information at the bottom of the form in the Analysis Pane. See [Working with Objects](#) for more information about forms.

Note the following:

- Look for one of the following at the bottom of the display area:



Open the Analysis Pane if necessary by clicking the  expand button.

- Place your mouse cursor over the title bar to display the  symbol, then resize as necessary.
- The Analysis Pane remains blank until an object is selected.
- If you select multiple objects or clear a selection, NNMi retains the Analysis Pane's contents.
- If you change views, NNMi clears the Analysis Pane.
- Click any  Refresh icon in the Analysis Pane to update a subset of displayed information.
- NNMi automatically refreshes the entire Analysis Pane's contents when you save a form.
- The Gauges tab shows real-time SNMP gauges to display State Poller and Custom Poller SNMP data.



- These gauges are displayed for Nodes, Interfaces, Custom Node Collections, and for Node Components of type CPU, Memory, Buffers, or Backplane.
- NNMi displays a gauge for each significant MIB Object Identifier (OID) that the node or interface supports, up to the default maximum of 24.

**Tip:** If you are an NNMi administrator, for information about using the `nms-ui.properties` file to change this default, see the "NNMi Console" chapter in the *HP Network Node Manager i Software Deployment Reference*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>.

- Each gauge displays the current OID value, using the default refresh rate of 15 seconds. (If you are an NNMi administrator, for information about using the `nms-ui.properties` file to change this default, see the "NNMi Console" chapter of the *HP Network Node Manager i Software Deployment Reference*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>.)
- The value range displayed indicates the OID minimum and maximum values that NNMi has encountered.
- For any gauge that tracks percentage values, NNMi uses a red line to indicate where the OID value is near 100 percent.
- There is not a one-to-one match between the OIDs used to analyze monitoring thresholds and those displayed in the Analysis Pane. For example, the Analysis Pane might display a **Cisco Memory Pool** OID value that does not match the value used to calculate whether the **Memory Utilization** Monitored Attribute threshold is reached or exceeded. This is because some threshold metrics require more complex calculations than a single OID allows.

**Tip:** If a gauge label appears to be a duplicate value, mouse over the label to view the more complete tooltip name that appears. (If you are an NNMi administrator, to change the gauge title from the NNMi component name to the SNMP MIB variable name, see the "Maintaining NNMi" chapter of the *HP Network Node Manager i Software Deployment Reference*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>.)

- To launch an SNMP Line Graph for the selected metric, click the icon that appears at the bottom of each gauge.
- To select and copy the tooltip information, double-click the gauge. NNMi opens a text window that enables you to select and copy the tooltip information.

#### Related Topics:

["Node Form" on page 50](#)


["Interface Form" on page 90](#)

["IP Address Form" on page 132](#)

## 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. Double-click the row representing the incident that you want to examine. See "Incident Form" on page 311.

### Related Topics:

[Using Views to Display Data](#)

[Working with Objects](#)

[Use Table Views](#)

## Export Maps to Microsoft® Visio (NNM iSPI NET)

### *NNM iSPI Network Engineering Toolset Software*

If you are using a map view to monitor your network, there are times when you might want to export topology maps displayed in NNMi to Visio documents for later use. NNMi enables you to export the current map or all Node Group maps that are configured to be exported. See "Help for Administrators" for more information about how to configure Node Group maps.

**Note:** Vendor-specific icons are not exported.

If you are using Internet Explorer as your Web browser, before exporting topology maps to Visio, make sure the NNMi management server is a trusted site and that File Downloads is enabled. Click [here](#) for more information.

### To add the NNMi management server as a trusted site:

1. Select **Tools** → **Internet Options**.
2. Navigate to the **Security** tab.
3. Select **Trusted Sites**.
4. Click **Sites**.
5. In the **Add this website to the zone** field, enter the url to the NNMi management server and click **Add**.
6. Click **OK** to save your changes and close the **Trusted Sites** dialog.

### To enable File Downloads:

1. Select **Tools** → **Internet Options**.
2. Navigate to the **Security** tab.
3. Select **Trusted Sites**.
4. Click **Custom Level**.
5. Navigate to the **Automatic prompting for file downloads**.
6. Select **Enable**.
7. Navigate to **File download**.
8. Select **Enable**.
9. Click **OK** to save your changes and close the **Security Settings** dialog.
10. Click **OK** to close the **Internet Options** dialog.

**To export the current map to a Visio diagram:**

1. Navigate to the map of interest. For example, select **Node Group Overview** from the **Topology Maps** workspace.
2. Select **Tools** → **Visio Export** → **Current Map**.
3. Select **Include Node Status Color** if you want to export the current Status color for each node.
4. Select **Include connection labels** if you want to export all of the connection labels.

**Note:** Including connection labels increases the file size. If you are concerned about file size, do not export the connection labels.

5. Click **OK**.
6. In the browser dialog, specify whether you want to Open or Save the .vdx file.

NNMi creates a Visio (.vdx) file that contains a single page with the current map view rendered as a Visio diagram.

**To export all Node Group maps configured to be exported:**

1. Select **Tools** → **Visio Export** → **Saved Node Group Maps**.

**Note:** Only those Node Group maps that have been properly configured by enabling the **Include in Visio Export** check box in the Node Group Map Settings form are included in the Visio Export. If a Node Group Map has not been saved using **Save Layout**, the positions of each node in the export will not match any changes you made in your Map view. See "[Position Nodes on a Node Group Map](#)" on page 257 for more information.

2. Select **Include Node Status Color** if you want to export the current Status color for each node.
3. Select **Include connection labels** if you want to export all of the connection labels.

**Note:** Including connection labels increases the file size. If you are concerned about file sizes, do not export the connection labels

4. Click **OK**

5. In the browser dialog, specify whether you want to Open or Save the .vdx file.  
NNMi creates a Visio (.vdx) file that contains a separate page for each Node Group map rendered as a Visio diagram.

### Related Topics

"Hide Connections or Connection Labels from an Exported Visio Diagram (NNM iSPI NET)" below

"View the Details for a Map Object on an Exported Visio Diagram (NNM iSPI NET)" on the next page

"Print an Exported Visio Diagram (NNM iSPI NET)" on the next page

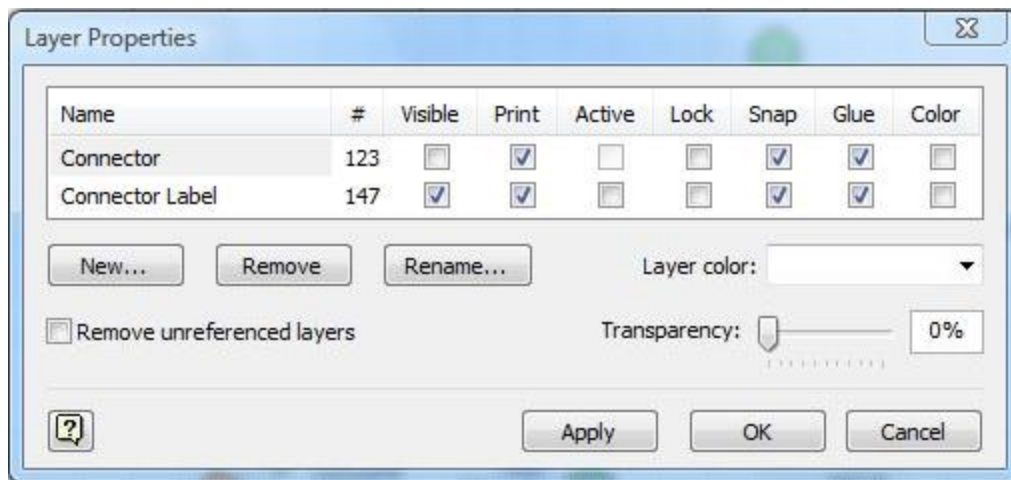
## Hide Connections or Connection Labels from an Exported Visio Diagram (NNM iSPI NET)

*NNM iSPI Network Engineering Toolset Software*

When viewing an NNMi topology map that was exported to Visio, you can temporarily hide the Connections or Connection Labels using the **View** menu.

**To hide the Connections or Connection Labels from a map that was exported to Visio:**

1. Open the Visio diagram of interest.
2. Select **View** → **Layer Properties**.
3. To hide the Connections from the Visio Diagram clear the check box that appears in the **Visible** column next to the **Connector** name as shown in the following example.



To hide the Connector Labels, clear the check box that appears in the **Visible** column next to the **Connector Label** name.

4. Click **Apply** to apply the changes.
5. Click **OK** to close the dialog.

### Related Topics

["Export Maps to Microsoft® Visio \(NNM iSPI NET\)" on page 290](#)

["View the Details for a Map Object on an Exported Visio Diagram \(NNM iSPI NET\)" below](#)

["Print an Exported Visio Diagram \(NNM iSPI NET\)" below](#)

## View the Details for a Map Object on an Exported Visio Diagram (NNM iSPI NET)

*NNM iSPI Network Engineering Toolset Software*

When viewing an NNMi topology map that was exported to Visio, you can view the details for a map object that is stored in the NNMi database using the **View** menu.

**To view the details for a map object on a map that was exported to Visio:**

1. Open the Visio diagram of interest.
2. Select the map object of interest.
3. Select **View** → **Shape Data Window**.

If the object is stored in the NNMi database, NNMi displays the details available for the selected object. This information is similar to the information displayed when using Quick View in NNMi.

### Related Topics

["Export Maps to Microsoft® Visio \(NNM iSPI NET\)" on page 290](#)

["Hide Connections or Connection Labels from an Exported Visio Diagram \(NNM iSPI NET\)" on the previous page](#)

["Print an Exported Visio Diagram \(NNM iSPI NET\)" below](#)

## Print an Exported Visio Diagram (NNM iSPI NET)

*NNM iSPI Network Engineering Toolset Software*

When printing an NNMi topology map that was exported to Visio, use the Visio **File** menu to make sure all of your map contents print to one page.

**To print a map exported to a Visio diagram:**

1. Open the Visio diagram of interest.
2. Select **File** → **Page Setup**.
3. Navigate to the **Print Setup** tab.
4. Click **Fit to sheet(s) across**.
5. Click **OK** to save your changes and close the Page Setup dialog.
6. Use the **File** → **Print** menu to print the Visio diagram.

### Related Topics

["Export Maps to Microsoft® Visio \(NNM iSPI NET\)" on page 290](#)

["Hide Connections or Connection Labels from an Exported Visio Diagram \(NNM iSPI NET\)" on page 292](#)

["View the Details for a Map Object on an Exported Visio Diagram \(NNM iSPI NET\)" on the previous page](#)

## Monitor with Line Graphs

The NNMi Actions menu enables you to view real-time SNMP data for selected nodes or interfaces. This feature is useful when you want to use a Line Graph to monitor a numeric MIB Expression value for a node or interface over a specified time interval. For example, you might want to view a Line Graph of the network traffic using the ifOutOctets (Interface Out Octets) MIB variable for a specified node. Or you might want to graph a MIB variable, such as ifInOctets (Interface In Octets), to verify that a problem has been fixed for a specified interface before closing an incident.

**Note:** The node for which you want to view information must support SNMPv1, SNMPv2c, or SNMPv3.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

NNMi provides a set of Line Graphs for nodes and for interfaces. See ["Line Graphs Provided by NNMi" on page 305](#) for more information.

Your NNMi administrator might configure additional Line Graphs.

### To access a Line Graph from a table view:

1. Navigate to the view for that object (for example, **Inventory** workspace, **Nodes** view).
2. Select the nodes or interfaces of interest by pressing CTRL-Click and selecting the rows representing the object information.
3. Select **Actions** → **Graphs** → <graph\_submenu> → <graph\_name>

**Note:** This menu item also is available on any supported object's form.

### To access a Line Graph from a map:

1. Navigate to the map of interest (for example, **Topology Maps** workspace, **Initial Discovery Progress** or **Network Overview** map).
2. Click the object or objects that have the data you want to graph.

**Tip:** Use CTRL-Click to select multiple objects.

3. Select **Actions** → **Graphs** → <graph\_submenu> → <graph\_name>

Your NNMi client displays the corresponding Line Graph and continues to request new values until you close the Line Graph window.

### Related Topics

"Using Line Graphs" below

## Using Line Graphs

The NNMi Line Graph enables you to view real-time SNMP data over time for selected nodes or interfaces.

Each line on a Line Graph represents a numeric value you want to monitor. For example, to enable you to monitor network traffic using a Line Graph, your NNMi administrator might configure a graph so that each line represents the ifOutOctets (Interface Out Octets) MIB variable value for an interface on a specified node. If more lines than the default number to be displayed on the graph are available, you can change the set of lines you want to view from the default selection.

**Note:** If NNMi displays a gap in a line on the graph, this means data was not available during the points in time indicated by the gap. Any line that discontinues in the Line Graph indicates the line no longer has available data.

**Tip:** If a Line Graph displays data as a different type than expected, contact your NNMi administrator. The NNMi administrator can override a MIB OID Type. If you are an NNMi administrator see [Override MIB OID Types](#) for more information.

**Note:** When the NNMi administrator overrides a MIB OID Type, you must restart the Line Graph for the configuration changes to take effect. After a Line Graph is restarted, the configuration changes are also displayed on any existing Line Graphs.

From a Line Graph, you perform the following tasks:

- ["Change the Lines Displayed on a Line Graph" below](#)
- ["Emphasize a Line Displayed on a Line Graph" on page 297](#)
- ["Hide a Line Displayed on a Line Graph" on page 297](#)
- ["Show and Hide the Line Graph Legend" on page 298](#)
- ["Change the Polling Interval for a Graph" on page 299](#)
- ["Select a Time Segment Using the Timeline Viewer" on page 299](#)
- ["Unlock the Y-Axis When Viewing a Time Segment" on page 300](#)
- ["Change the Zoom Value for a Graph" on page 301](#)
- ["Display Data Values on a Graph" on page 301](#)
- ["Display Messages on a Line Graph" on page 302](#)
- ["Determine the Maximum Time Range for a Graph" on page 303](#)
- ["Print a Graph" on page 303](#)
- ["Export Graph Data to a Comma-Separated Values \(CSV\) File" on page 304](#)

## Change the Lines Displayed on a Line Graph

When you display a Line Graph, you must first select the nodes or interfaces for which you want to graph information. See ["Monitor with Line Graphs"](#) on the previous page for more information about accessing a Line Graph.

In response, NNMi creates a line for each numeric value defined for the graph. For example, to monitor network traffic, your NNMi administrator might configure a graph so that each line represents the ifOutOctets (Interface Out Octets) MIB value for an interface on a specified node.

By default, NNMi displays up to 20 lines of data at one time. If more than 20 instances of data are available, NNMi uses the notification area to inform you that the number of lines to be displayed exceeds your default number. See ["Display Messages on a Line Graph" on page 302](#) for more information about the notification area.

**Note:** The NNMi administrator can change the default number of lines to be initially displayed.

See the legend provided with each graph for information about the data represented by each line color on the graph.

NNMi enables you to change which lines are displayed in a Line Graph. For example, if you select a graph that displays ifOutOctets (Interface Out Octets) MIB values for all of the interfaces on a node, you can choose to display only the interfaces with the most traffic.

You can also hide lines displayed on a graph. When a line is hidden, NNMi continues to request new data for that instance. See ["Hide a Line Displayed on a Line Graph" on the next page](#) for more information.

**To add a line to the Line Graph:**

1. Select **File** → **Select Lines...**

NNMi displays the Select Lines dialog box.

2. In the **Select Lines** dialog box, do one of the following:

- To display a line for one or more instances of data that appear in the Select Lines dialog box, select the check box  in the row representing each instance of data that has a line you want to display.
- To display lines for all instances of data that appear in the Select Lines dialog box, select the check box () that appears above the check box column.

3. Click **OK**.

The Line Graph displays the new set of lines specified.

**To remove a line on the Line Graph:**

**Note:** If a line is removed from the Line Graph, NNMi no longer tracks the SNMP data for that instance.

1. Select **File** → **Select Lines...**

NNMi displays the Select Lines dialog box.

2. In the **Select Lines** dialog box, do one of the following:

- To remove a line for one or more instances of data, deselect the check box () in the row representing each instance of data that has a line you want to remove.
- To clear all lines for all instances of data that appear in the Select Lines dialog box, deselect the check box () that appears above the check box column.



**Note:** If only some instances of data are selected, click the check box above the check box column twice. The first click selects all instances of data and the second click clears the check box for all data instances.

3. Click **OK**.

The Line Graph displays the new set of lines specified.

## Emphasize a Line Displayed on a Line Graph

NNMi enables you to emphasize a line displayed in a Line Graph.

### To emphasize a line on the Line Graph:

1. Navigate to the Graph Legend.

**Note:** if the Legend is not displayed, select **View** → **Legend**.

2. Mouse over the legend entry representing the line that you want to emphasize.

The selected legend entry appears bold and all other lines fade.

## Hide a Line Displayed on a Line Graph

NNMi enables you to temporarily hide lines displayed in a Line Graph. For example, if you select a graph that displays ifOutOctets (interface Out Octets) MIB variable values for all of the interfaces on a node, you can choose to display only the interfaces with the most traffic and hide those interfaces with the least traffic.

You can also choose to hide a line containing extreme values so that the Y-axis is recalculated to show more detail for the remaining lines.

**Note:** NNMi continues to request new data for instances with hidden lines. A line that was hidden can be added back to the graph at any time and display the most current information.

### To hide a line on the Line Graph:

1. Navigate to the Graph Legend

**Note:** if the Legend is not displayed, select **View** → **Legend**.



2. Click the entry in the Legend representing the line that you want to hide.



3. Click the popup text to hide the line.



4. The line entry disappears from the map and the Legend link text turns gray.

**To display a line that is hidden:**

1. Navigate to the Graph Legend.

**Note:** if the Legend is not displayed, select **View** → **Legend**.

2. Hidden line entries have gray text in the Legend.

Click the entry in the Legend representing the hidden line that you want to display.



3. Click the popup text display the line.



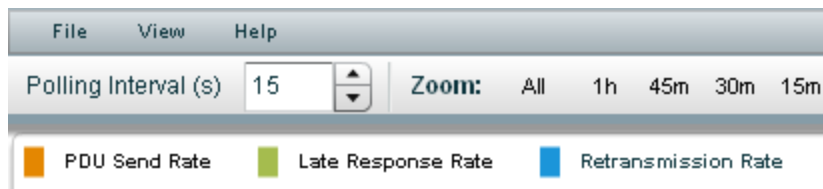
4. The line entry appears on the map and the Legend link text turns black.

You can also remove a line from the Line Graph. When you remove a line from the Line Graph, NNMi stops requesting new data for that instance. See "[Change the Lines Displayed on a Line Graph](#)" on page 295 for more information.

## Show and Hide the Line Graph Legend

The Graph Legend identifies each line displayed in the Line Graph. By default, NNMi displays the name of the node or interface for each line. If the graph displays more than one line per node, the legend includes the node name followed by the instance identifier specified by the NNMi administrator who configured the Line Graph. For example, the Interface Index (ifIndex) value might be used to identify each interface per node.

NNMi enables you to temporarily hide the legend displayed in a Line Graph. For example, if you need more than the default number of lines, you might want to hide the legend to provide more space to display the graph.



**To hide the legend on a Line Graph:**

Select **View** → **Legend**.

The check mark no longer appears next to the **Legend** menu option.

The legend no longer appears in the Line Graph.

**To redisplay a legend that is hidden:**

Select **View** → **Legend**.

The check mark re-appears next to the **Legend** menu option.

The legend reappears in the Line Graph.

## Change the Polling Interval for a Graph

The Polling Interval determines how often NNMi requests for the data point sets displayed in a graph. When you change the Polling Interval in a graph, you are temporarily changing the Polling Interval for graphing purposes only.

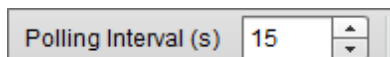
By default, NNMi uses 15 seconds, or a value specified by the NNMi administrator or HP Network Node Manager i Software Smart Plug-in.

**Note:** The NNMi administrator or HP Network Node Manager i Software Smart Plug-in specifies the Maximum Time Range in which to retain the graph's data point sets. After the Maximum Time Range number is reached, NNMi begins to discard the oldest data point sets so that it can display the most recent data for the time range specified. For example, if the Maximum Time Range is 24 hours, when 24 hours has passed, NNMi removes data starting with the initial data point set so that it can display data for the most recent 24-hour interval. NNMi displays a Warning message if it is unable to graph the data for the Maximum Time Range specified. You can lengthen the Polling Interval to lengthen the time period in which to retain the data. The time period in which the data is retained will not exceed the Maximum Time Range configured for the graph. See "[Determine the Maximum Time Range for a Graph](#)" on [page 303](#) for more information.

**Tip:** To pause a graph, set the Polling Interval to 0 (zero).

**To change the Polling Interval for a graph:**

1. In the **Polling Interval (secs)** attribute, type the number that represents how often you want NNMi to request new data point sets.



The image shows a user interface element for setting the polling interval. It consists of a text box containing the number '15', followed by a small vertical spinner control with up and down arrows.

2. Press **Enter**.

**Note:** The new Polling Interval takes effect after the next data display. For example, if you change the Polling Interval from 1 minute to 15 seconds, the graph waits until the 1-minute interval is completed, displays the additional data, and then begins waiting 15 seconds between data requests.

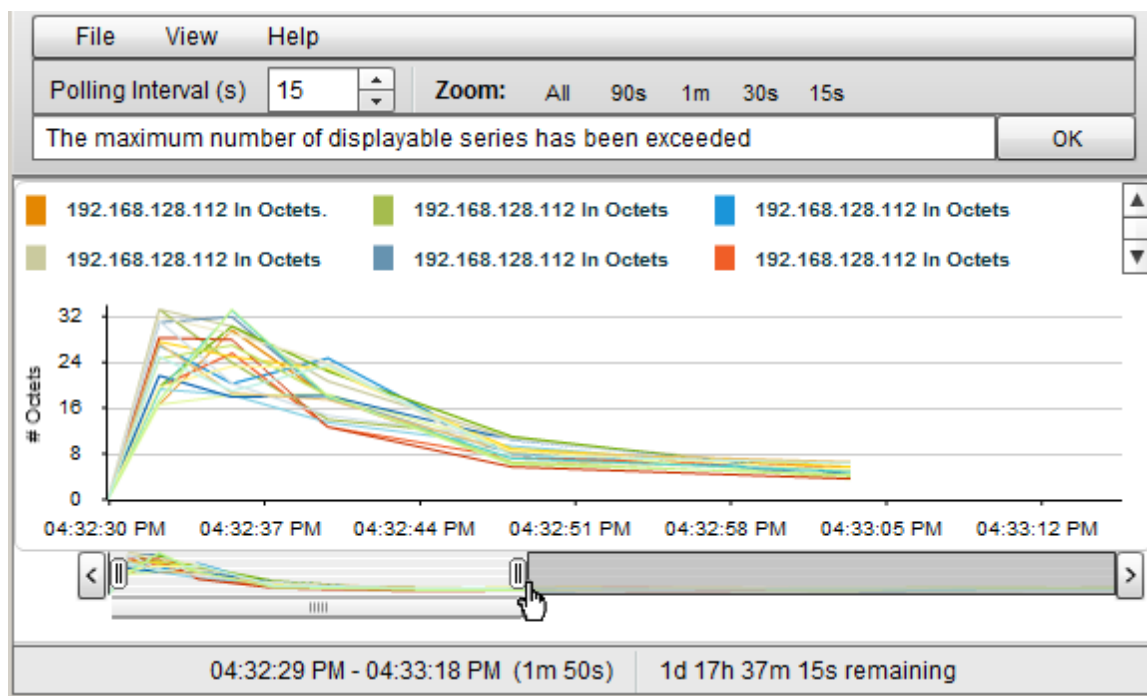
## Select a Time Segment Using the Timeline Viewer

NNMi enables you to pan to a specified time segment of the graph using the Timeline Viewer that appears below the graph.

**Note:** You can also use the Zoom factor to select a time segment. See "[Change the Zoom Value for a Graph](#)" on [page 301](#) for more information.

For example, you might want to focus on a particular day or a particular peak period. The following example uses the Timeline Viewer to select the most recent time segment available on the graph.

If the Timeline Viewer is not displayed, select **View** → **Timeline Viewer**.



**Note:** As shown in the example above, the Timeline highlights the section of the data that you chose to display in the graph and continues to display all of the data available.

**To select a time segment on a graph:**

**Note:** NNMI displays the timestamp of the time segment end point as you move the slider.

1. Move the left side of the slider in the Timeline to indicate the beginning of the section you want to display.
2. Move the right side of the slider in the Timeline to indicate the end of the section you want to display.

NNMI displays the results of your selection in the graph as shown in the previous example.

## Unlock the Y-Axis When Viewing a Time Segment

By default, NNMI locks the Y-axis so that it remains fixed at the minimum and maximum values for the current set of data regardless of the time segment selected. This means NNMI does not automatically re-adjust the Y-axis to match the data values for the selected time segment.

You can choose to unlock the Y-axis so that NNMI automatically adjusts the increments on the Y-axis. As the data values change, all of the data points fit on the graph. When using the Timeline Viewer to focus on a specified time segment, NNMI also automatically re-adjusts the increments on the Y-axis as new data is received.

For example, suppose the minimum value for the current data set is 0 and the maximum value is 20. In this case the Y-axis increments would range from 0 to 20. If you select a time segment in which the data points range from 0 to 5 and you lock the Y-axis, the increments remain fixed at 0 to 20. If

you unlock the Y-axis, NNMi automatically adjusts the Y-axis increments from 0 to 5 and enlarges the graph accordingly.

This option is useful when you have a wide range of data and you are viewing a series of time segments.

**Note:** By default, the **Lock Y-Axis** option is on.

**To unlock the Y-axis when viewing time segments of the graph:**

Select **View** → **Lock Y-Axis**

The check mark no longer appears next to the Lock Y-axis option to indicate the Y-axis is not locked.

**To lock the Y-axis when viewing time segments of the graph:**

Select **View** → **Lock Y-Axis**

A check mark appears next to the Lock Y-axis menu option to indicate the Y-axis is locked.

## Change the Zoom Value for a Graph

NNMi enables you to change the Zoom number on a graph. For example, you might want to focus on a specified time interval that indicates peak traffic for a node or interface.

**Note:** You can also move the slider in the Timeline Viewer that appears below the graph to zoom in on the area in which you want to focus. See "[Select a Time Segment Using the Timeline Viewer](#)" on page 299 for more information.

**To change the Zoom for a graph:**

Select one of the Zoom numbers displayed in the top of the graph.

In the following example the Zoom choices are All, 5 minutes (5m), 3 minutes (3m), 2 minutes (2m), and 90 seconds (90s):



Note the following:

- The All value displays all of the data available.
- The Zoom values might change depending on the Polling Interval specified.

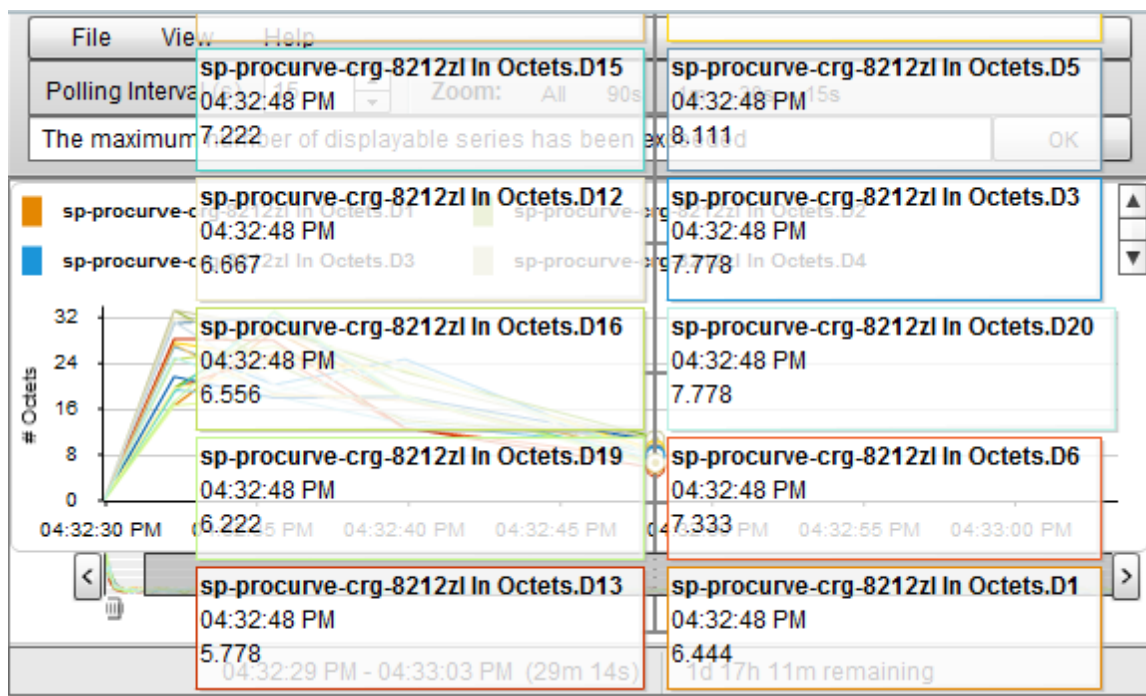
## Display Data Values on a Graph

An NNMi graph enables you to display data values at any point in time represented in the graph.

**To display data values at a specified point in time:**

Mouse over the location of interest.

NNMi displays the numeric value for each graphed object at the point selected as shown in the following example:



## Display Messages on a Line Graph

An NNMI Line Graph enables you to display the history of messages generated for a particular graph. Messages can be either informational or warning messages that result when NNMI is unable to display a particular line in the graph. For example, an SNMP timeout might prohibit NNMI from displaying updated data.

NNMI also displays a Warning message if it is unable to graph the data for the Maximum Time Range specified. See "Determine the Maximum Time Range for a Graph" on the next page for more information.

You can also control whether NNMI automatically displays the Message History dialog box in a pop-up window each time NNMI receives a new Warning message.

### To display the history of messages:

1. Select **View** → **Notification History**.

NNMI displays the Date, Type (Info or Warning) and Description for all messages that you have not deleted.

2. Click **Delete History** to delete the list of messages displayed.

**Note:** Any messages deleted from the Notification History are no longer available for viewing.

3. Click **OK** to close the Notification History dialog box.

**To control whether the Notification History dialog box is automatically displayed in a pop-up window each time NNMI receives a new Warning message:**

1. Select **View** → **Notification History**.
2. Do one of the following:
  - Select to clear  **Show on warning** if you do not want NNMI to automatically display Warning messages in a Status pop-up window.
  - Select to check  **Show on warning** to display Warning messages in a pop-up window as they occur.

NNMI displays individual messages in a notification area that appears above the graph when a message occurs. To clear a message displayed in the notification area, click the **OK** button that appears to the right of the message. The message remains available to be displayed when using Notification History.

## Determine the Maximum Time Range for a Graph

The NNMI administrator specifies the Maximum Time Range in which the data in a graph should be retained. After the Maximum Time Range number is reached, NNMI discards the oldest data point sets so that it can display the most recent data for the time range specified. For example, if the Maximum Time Range is 24 hours, when 24 hours has passed, NNMI removes data starting with the initial data point set so that it can display data for the most recent 24-hour interval.

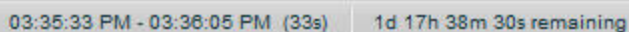
To determine the Maximum Time Range for a graph use the graph status bar. The status bar displays the following information:

- The start and end time indicating the time interval in which data has been collected for the graph. NNMI updates this time at each Polling Interval.

**Note:** Any time NNMI removes older data from the graph, the start time in which data has been collected for the graph changes to indicate the new start time.

- The total time in which data has been collected for the graph.
- The time remaining before the Maximum Time Range is reached.

In the following example, the total time in which data has been collected for the graph is 33 seconds (33s). The time remaining before the Maximum Time Range is reached is 1 day, 17 hours, 38 minutes, and 30 seconds (1d 17h 38m 30s remaining)



03:35:33 PM - 03:36:05 PM (33s) 1d 17h 38m 30s remaining

**Note:** NNMI displays a Warning message if it is unable to graph the data for the Maximum Time Range specified. You can increase the Polling Interval to lengthen the time period in which the data remains current. The time period in which the data remains current will not exceed the Maximum Time Range configured for the graph.

## Print a Graph

NNMI enables you to print a graph using the graphs's File menu. NNMI automatically scales all information included in the graph window to fit the printed page.

**To print a graph:**

Select **File** → **Print** to access the Print dialog box and send the graph contents to the designated printer.

## Export Graph Data to a Comma-Separated Values (CSV) File

NNMi enables you to export a Line Graph to a Comma-Separated Values (CSV) file. NNMi exports the data collected only for the lines displayed on the graph. (To change the lines displayed use the **File** → **Select Lines** option.)

**To export a graph to a CSV file:**

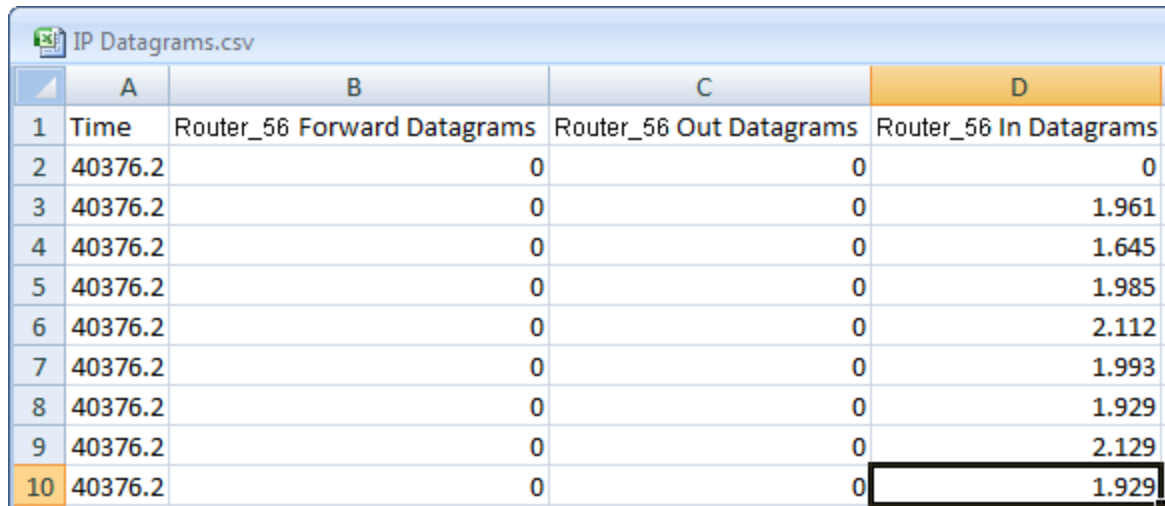
1. Display the Line Graph that contains the data you want to export. (See "Monitor with Line Graphs" on page 294.)
2. Select **File** → **Export to CSV** .

NNMi uses the graph Name as the .csv file name.

3. Click **Save** to save the file.

As shown in the following example, NNMi creates the CSV file using the following format:

- The first column lists each time stamp in which data is collected.
- Each row contains the data per line for the specified time.
- Each column represents a line in the graph.



	A	B	C	D
1	Time	Router_56 Forward Datagrams	Router_56 Out Datagrams	Router_56 In Datagrams
2	40376.2	0	0	0
3	40376.2	0	0	1.961
4	40376.2	0	0	1.645
5	40376.2	0	0	1.985
6	40376.2	0	0	2.112
7	40376.2	0	0	1.993
8	40376.2	0	0	1.929
9	40376.2	0	0	2.129
10	40376.2	0	0	1.929

Note the following:

- By default, NNMi exports the time as a decimal value. This number represents the number of days since Jan 1, 1900. To format the time as a date value, in the CSV file, right-click the **Time** column, select **Format Cells**, and select **Date**.
- Blank or null values indicate that NNMi was unable to collect data from the device.



- A value of 0 (zero) represents a valid value collected from the device for the specified timestamp.

## Line Graphs Provided by NNMi

NNMi provides a set of Line Graph that display real-time SNMP data for specified MIB Expressions. These Line Graphs are available from the **Actions** → **Graphs** submenu.

Your NNMi administrator might configure additional Line Graphs that also appear under the Actions menu.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

### To display the Line Graphs available for nodes:

1. Navigate to the node view of interest (for example, **Inventory** workspace, **Nodes** view).
2. Press CTRL-Click and select each row that represents a node you want to graph.
3. Select **Actions** → **Graphs** → <graph\_submenu> → <graph\_name>.
4. Some Line Graphs are specific to a vendor or object type. If the required object or objects are not selected, the color of that Action is gray to indicate the Action is unavailable.

### To display the list of Line Graphs available for interfaces:

1. Navigate to the interface view of interest (for example, **Inventory** workspace, **Interfaces** view).
2. Press CTRL-Click and select each row that represents an interface you want to graph.
3. Select **Actions** → **Graphs** → <graph\_submenu> → <graph\_name>.

Some Line Graphs are specific to a vendor or object type. If the required object or objects are not selected, the color of that Action is gray to indicate the Action is unavailable.

### To display the Line Graph available for an incident:

1. Navigate to the incident view of interest (for example, **Incident Browsing** workspace, **Root Cause Incidents** view).
2. Select the row that represents the incident of interest.

**Note:** Select only one incident. The Source Node of the incident you select must be associated with a Custom Poller Collection.

3. Select **Actions** → **Graphs** → **Graph Custom Poller Results**.

NNMi displays a Line Graph for the incident you select. See "[Display a Line Graph from an Incident \(Custom Poller Only\)](#)" on the next page for more information about the Line Graph displayed.

### To display the Line Graph available for Custom Polled Instances:

1. Navigate to the **Monitoring** workspace, **Custom Polled Instances** view.
2. Press CTRL-Click and select each row that represents a Custom Polled Instance you want to graph.
3. Select **Actions** → **Graphs** → **Graph Polled Instance**.

NNMi displays a Line Graph that includes the data for each Custom Polled Instance you select. See ["Display a Line Graph for a Custom Polled Instance"](#) on the next page for more information about the Line Graph displayed.

**Note:** You can also access Line Graphs from an object's form.

See ["Monitor with Line Graphs"](#) on page 294 for more information about accessing Line Graphs.

## Display a Line Graph from an Incident (Custom Poller Only)

If you are using incident views to monitor your network, you might want to switch to a Line Graph to determine more information about an incident that is associated with a Custom Poller Collection. This means the incident's Source Node is a member of a Node Group for which a Custom Poller Policy is defined.

NNMi graphs MIB expressions from the Custom Poller Collection associated with the incident's Source Node. See ["About Custom Poller"](#) for more information about Custom Poller and Custom Poller Collections.

You can identify a Custom Poller incident in either of the following ways:

- The incident's Message includes the keywords: `for variable`.
- The CIAs listed on the Incident form's Custom Attributes tab, include the following Custom Poller attributes:
  - `cia.custompoller.collection`
  - `cia.custompoller.instanceDisplayValue`
  - `cia.custompoller.instanceFilterValue`
  - `cia.custompoller.lastValue`
  - `cia.custompoller.mibInstance`
  - `cia.custompoller.policy`
  - `cia.custompoller.state`
  - `cia.custompoller.variable.description`
  - `cia.custompoller.variable.expression`
  - `cia.custompoller.variable.name`
  - `com.hp.ov.nms.apa.symptom`

**To display an Line Graph from an incident view:**

1. Navigate to the incident view of interest (for example, **Incident Browsing** workspace, **Root Cause Incidents** view).
2. Select the row that represents the Custom Poller incident of interest.  
**Note:** Select only one incident.
3. Select **Actions** → **Graphs** → **Graph Custom Poller Results** in the main toolbar.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

NNMi displays a Line Graph that contains the data points for the MIB expression configured for the Custom Poller Collection associated with the incident's Source Node. See "[Using Line Graphs](#)" on page 295 for more information.

**To display an Line Graph from an incident form:**

1. Navigate to the incident view of interest (for example, **Incident Browsing** workspace, **Root Cause Incidents** view).
2. Double-click the row representing the incident that has the Custom Poller results you want to graph.
3. Select **Actions** → **Graphs** → **Graph Custom Poller Results** in the main toolbar.

NNMi displays an Line Graph that contains the lines representing the data points for the MIB expression configured for the Custom Poller Collection associated with the incident's Source Node. See "[Using Line Graphs](#)" on page 295 for more information.

## Display a Line Graph for a Custom Polled Instance

If you are using the Polled Instance view to monitor your network, you might want to switch to an Line Graph to determine more information about a particular Custom Polled Instance.

NNMi graphs the line representing the Custom Poll results for the selected Custom Polled Instance. See "[About Custom Poller](#)" for more information about Custom Poller

**To display an Line Graph from the Custom Polled Instance view:**

1. Navigate to the **Custom Polled Instances** view (**Monitoring** workspace, **Custom Polled Instances** view).
2. Press CTRL-Click and select each row that represents the Custom Polled Instance of interest.
3. Select **Actions** → **Graph Polled Instance** in the main toolbar.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

NNMi displays a Line Graph that includes the data for each Custom Polled Instance you select.

**To display an Line Graph from a Custom Polled Instance form:**

1. Navigate to the **Custom Polled Instances** view (**Monitoring** workspace, **Custom Polled Instances** view).

2. Double-click the row representing the Custom Polled Instance that has data that you want to graph.
3. Select **Actions** → **Graph Polled Instance** in the main toolbar.  
NNMi displays a Line Graph that includes the data for each Custom Polled Instance you select.

**Related Topics**

["Custom Polled Instances View" on page 282](#)

# Chapter 8

## Monitoring Incidents for Problems

**Tip:** See "Incident Form" on page 311 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.

**Note:** NNMi enables an NNMi administrator to limit visibility and control to parts of the network for some or all operators. If your NNMi administrator has configured Security Groups to limit node access, then as a network operator you can view a node and its associated incidents only if one of the User Groups to which you belongs is associated with that node's Security Group. See "Node and Incident Access" on page 19 for more information.

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, Lifecycle State, source node, source object, and its message.

**Note:** Some incidents might have the Source Node or Source Object value set to **<none>**. This happens when the NNMi database does not contain any object representing the problem device. Examples: An incident that is being forwarded from an NNM 6.x or 7.x management station has a Source Node value of **<none>**. An incident having a Source Node or Source Object that is not included in the current NNMi Monitoring Configuration settings 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 can set some of these management mode attribute values. Any object that has a management mode that 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	<p>Within a view, each incident has a corresponding icon that indicates its severity so that you are immediately notified of potential or current problems.</p> <p>You can filter incidents so that you only view incidents that has a severity that is Critical or you can choose to filter incidents to view all incidents that have a severity that is greater than Normal.</p>
Identify problem nodes	You can sort incidents by node to help you quickly identify the problem nodes.
Determine the cause of the problem	<p>You can sort an incident view by description, to see all incidents reporting a node or interface that is disabled or otherwise unavailable.</p> <p>You can also use the child incidents attribute to view all of the incidents that are a result of the root cause problem reported.</p>
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 incidents important 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 that have a status that 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="#">"Filter Views by Node or Interface Group"</a> on page 26 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.

**Note:** If a node is deleted, only an NNMi administrator can view the incidents associated with that node.

### Tasks Performed from an Incident View

You can perform the following tasks from an incident view:

"Organize Your Incidents" below

"Own Incidents" on page 331

"Assign Incidents" on page 332

"Unassign Incidents" on page 333

"Keep Your Incidents Up to Date" on page 334

"Track an Incident's Progress" on page 336

"Display a Map from an Incident" on page 337

### Related Topics:

"Incident Views Provided by NNMi" on page 340

## 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 can 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 "[Filter Views by Node or Interface Group](#)" on page 26 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


















**Tip:** See "[Interpret Root Cause Incidents](#)" on page 387 for additional information about troubleshooting an incident.

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 permits, you can use this form to update the [priority](#) and [Lifecycle 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	<p>Seriousness that NNMi calculates for the incident. Possible values are:</p> <ul style="list-style-type: none"> <li> No Status</li> <li> Normal</li> <li> Warning</li> <li> Minor</li> <li> Major</li> <li> Critical</li> <li> Disabled</li> <li> Unknown</li> </ul> <p>See <a href="#">About Status Colors</a> for more information about severity values.</p> <p><b>Note:</b> The icons are displayed only in table views.</p>
Priority	<p>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:</p> <ul style="list-style-type: none"> <li> 5 None</li> <li> 4 Low</li> <li> 3 Medium</li> <li> 2 High</li> <li> 1 Top</li> </ul> <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> <ul style="list-style-type: none"> <li> <b>Registered</b> – Indicates that an incident arrived in the queue stored in the NNMi database.</li> <li> <b>In Progress</b> – State selected by someone on your team to indicate that they are taking responsibility for investigating the problem.</li> <li> <b>Completed</b> – State selected by someone on your team to indicate completion of the incident investigation and implementation of a solution.</li> <li> <b>Closed</b> – Indicates that NNMi determined 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.</li> </ul>



**Basic Attributes, continued**









Attribute	Description
	<p><b>Note:</b> NNMi does not automatically Close incidents whose Correlation Nature is <b>Info</b>. These incidents are meant to provide information regarding changes in your network that might be of interest. You will need to Close these incidents if you do not want them to remain in your incident queue. See "<a href="#">Incident Form: General Tab</a>" on the next page for more information about Correlation Nature</p> <p> <b>Dampened</b> – Indicates that, within the configured <i>acceptable time period</i>, NNMi determined the problem reported by this Incident is no longer a problem. NNMi does not submit the incident to the queue until after the time period (configured by the NNMi administrator).</p> <p>In some cases, NNMi updates an incident's Lifecycle State for you. See "<a href="#">About the Incident Lifecycle</a>" on page 335 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>The Name attribute value of the node associated with the incident. Click the  Lookup icon and select  Show Analysis or  Open to display the "<a href="#">Node Form</a>" on page 50 for more information about the node.</p> <p><b>Note:</b> If the NNMi database does not contain any Node object for this device, 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 will 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  Show Analysis 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</a>" on page 331 for more information.</p>
Notes	<p><i>(NNMi Advanced - Global Network Management feature)</i> The text you enter here is not sent from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager can add notes that are stored in the NNMi database on the Global Manager.</p> <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, spaces, and special characters (~ ! @ # \$ % ^ &amp; * ( ) _ + -) are permitted.</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 311 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 an exceeded threshold. For example, a utility exceeds 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 occurred on a device. For example, when a Cisco device powers up or powers down.</li></ul> <p><b>Note:</b> The icons are 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></ul>

















### General Attributes, continued

Attribute	Description
	 <b>Aggregated Port</b> – Indicates the incident is related to a <a href="#">Link Aggregation</a> <sup>1</sup> problem. See "Interface Form: Link Aggregation Tab (NNMi Advanced)" on page 98.
	 <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.
	 <b>Board</b> - Indicates the incident is related to a board problem. This family is not used by NNMi with default configurations, but it is available for incidents you define.
	 <b>Chassis</b> – Indicates the incident is related to an chassis problem. This family is not used by NNMi with default configurations, but it is available for incidents you define.
	 <b>Component Health</b> – Indicates the incident is related to Node Component metrics collected by NNMi. See "Node Form: Node Components Tab" on page 69 for more information about the Node Component metrics collected.
	 <b>Connection</b> – Indicates the incident is related to a problem with one or more connections.
	 <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.
	 <b>Custom Poller</b> – Indicates the incident is related to the NNMi Custom Poller feature. See "About Custom Poller".
	 <b>HSRP</b> – <i>NNMi Advanced</i> . Indicates the incident is related to a Hot Standby Router Protocol ( <a href="#">HSRP</a> <sup>2</sup> ) problem.
	 <b>Interface</b> – Indicates the incident is related to a problem with one or more interfaces.
	 <b>License</b> - Indicates the incident is related to a licensing problem.
	 <b>NNMi Health</b> – Indicates the incident is related to NNMi Health. See the <a href="#">Check NNMi Health</a> for more information.

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.









<sup>2</sup>Hot Standby Router Protocol

### General Attributes, continued



Attribute	Description
	<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 a Router Redundancy Protocol configuration 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>Syslog</b> – NNMi does not use this Family with default configurations. 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>VLAN</b> – Indicates the incident is related to a problem with a virtual local area network.</p> <p> <b>VRRP</b> – <i>NNMi Advanced</i>. Indicates the incident is related to a Virtual Router Redundancy Protocol (<b>VRRP</b><sup>1</sup>) problem.</p> <p><b>Note:</b> The icons are only in table views.</p>
Origin	<p>Identifies how the incident was generated. Possible values are:</p> <p> <b>NNMi</b> – Indicates the incident was generated by NNMi processes.</p> <p> <b>Manually Created</b> – NNMi does not use this Origin with default configurations. It is available for incidents you define.</p> <p> <b>NNM 6.x/7.x</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>Syslog</b> – NNMi does not use this Origin with default configurations. It is available for incidents you define.</p> <p> <b>Other</b> – Indicates the incident was generated by a source other than the Origin</p>

<sup>1</sup>Virtual Router Redundancy Protocol




### General Attributes, continued

Attribute	Description
	<p>categories provided.</p> <p><b>Note:</b> The icons are 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>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 primary problem. Secondary Root Cause Incidents are the Child Incidents of Parent Incidents and often begin as primary Root Cause incidents. Whenever a primary Root Cause Incident is correlated under another Incident, its Correlation Nature becomes Secondary Root Cause. Click here for more information.</p> <p>For example, if an <b>Interface Down</b> incident is followed by a <b>Node Down</b> Incident on a neighboring device, the <b>Interface Down</b> Incident becomes a Child Incident to the Parent <b>Node Down</b> incident. Its Correlation Nature becomes Secondary Root Cause.</p> <p>Use the All Incidents view to examine both Secondary Root Cause and primary Root Cause Incidents. Use the Root Cause view to see only the primary Root Cause Incidents. In the Root Cause Incidents view, any Secondary Root Cause Incident is correlated under its associated primary Root Cause Incident.</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>Service Impact</b> - Indicates a relationship between incidents in which a network service is affected by other incidents. For example, an Interface Down incident can affect a Router Redundancy Group that is part of an HSRP service. This Correlation Nature is available for use by HP Network Node Manager i Software Smart Plug-ins (iSPIs). See "Help for Administrators" for more information about NNM iSPIs.</p> <p> <b>Stream Correlation</b> – <i>Used in NNMi 8.xx only.</i> 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) and Rate (occurrence of events by time).</p> <p> <b>None</b> – Indicates there is no incident correlation for the incident.</p> <p> <b>Info</b> – Indicates the incident is informational only.</p> <p> <b>Dedup Stream Correlation</b> – Stream correlations are created as NNMi</p>

**General Attributes, continued**

Attribute	Description
	<p>analyzes events and traps to determine the root cause incident for a problem. Dedup Stream Correlation indicates the Incident is a Deduplication Incident. Click here for more information.</p> <p>Deduplication Incident configurations determine what values NNMi should match to detect when an Incident is a duplicate. Duplicate Incidents are listed under a Duplicate Correlation Incident. NNMi tracks the number of duplicates generated. This value is captured as the Duplicate Count attribute and is incremented on the Duplicate Correlation Incident.</p> <p> <b>Rate Stream Correlation</b> – Stream correlations are created as NNMi analyzes events and traps to determine the root cause incident for a problem. Rate Stream Correlation indicates the Incident is a Rate Incident. Click here for more information.</p> <p>Rate Incidents track incident patterns <i>based on the number of incident reoccurrences within a specified time period</i>. After the count within the specified time period is reached, NNMi emits a Rate Correlation Incident and continues to update the Correlation Notes with the number of occurrences within that rate.</p> <p><b>Note:</b> The icons are only in table views.</p>
Duplicate Count	<p>Lists the number of duplicate incidents that NNMi encountered for the selected incident. This number increments in the associated deduplication incident that NNMi generates to inform the operator of incidents needing attention. The incidents are reoccurring according to the deduplication criteria specified in the incident's deduplication configuration.</p> <p>For example, by default, incidents generated from SNMP traps will not have their deduplication count incremented. If the NNMi administrator defines a deduplication criteria 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 <b>Lifecycle State</b>. 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 335 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>SNMP Trap Configuration, Remote NNM 6.x/7.x Event Configuration, or Management</b></li> </ul>

**General Attributes, continued**

Attribute	Description
RCA Active	<p><b>Event Configuration</b> form available from the <b>Configuration</b> workspace.</p> <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> <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 incident's <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 Lifecycle State 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> <li>• The time measured between when NNMi detected a problem with one or more network devices to the time the problem was resolved.</li> <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	<p>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 that has a rate criteria that was met.</p>

### General Attributes, continued

Attribute	Description
Last Occurrence Time	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 that has a rate criteria that was met.  If there are no duplicate incidents or incidents that have a rate criteria that were met, this date is the same as the First Occurrence Time.
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.

## Incident Form: Correlated Parents Tab

The "Incident Form" on page 311 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.  Double-click the row representing an incident. The Incident Form displays all details about the selected incident.

## Incident Form: Correlated Children Tab

The "Incident Form" on page 311 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.  Double-click the row representing an incident. The Incident Form displays all details about the selected incident.



## Incident Form: Custom Attributes Tab

The "Incident Form" on page 311 provides details for troubleshooting purposes.

For information about each tab:

**Note:** NNMi lists the Custom Attributes for incidents in the order in which they are received from the SNMP trap. If you sort or filter the Custom Attribute table, click the  Restore Default Settings icon to restore the Custom Attribute order for the selected incident.

(NNMi Advanced - Global Network Management feature) The NNMi administrator for the Global Manager can configure Custom Incident Attributes in addition to the ones that appear on the Regional Manager. If you are an NNMi administrator, see [Enrich Incident Configurations](#) for more information.

### Custom Attributes Table

Attribute	Description
Custom Incident Attributes	<p>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.</p> <p>Double-click the row representing the Custom Incident Attribute that has the "Custom Incident Attribute Form" below you want to see. For more information, see "Custom Incident Attributes Provided by NNMi (Information for Operators)" on the next page.</p>

## 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.

(NNMi Advanced - Global Network Management feature) The NNMi administrator for the Global Manager can configure Custom Incident Attributes in addition to the ones that appear on the Regional Manager. If you are an NNMi administrator, see [Enrich Incident Configurations](#) for more information.

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, double-click the row representing an incident. The "Incident Form" on page 311 displays all details about the selected incident.

2. In the **Incident** form, select the **Custom Attributes** tab.
3. Double-click the row representing the Custom Incident Attribute (CIA) 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>The Custom Incident Attribute (CIA) name limit is 80 characters. If this limit is exceeded, NNMi truncates the value from the left.</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, NNMi might provide 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> <p>The Custom Incident Attribute value limit is 2000 characters. If this limit is exceeded, NNMi truncates the value from the right.</p>

#### Related Topics:

["Custom Incident Attributes Provided by NNMi \(Information for Operators\)" below](#)

## Custom Incident Attributes Provided by NNMi (Information 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" on page 311, 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.

Some of the potential custom incident attributes provided by NNMI are described in the table below. If you are an NNMI administrator, also see [Custom Incident Attributes Provided by NNMI \(for Administrators\)](#).

**Custom Incident Attributes Provided by NNMI**

Name	Description
cia.address	SNMP agent address.
cia.incidentDurationMs	<p>The time measured in milliseconds between when NNMI detected a problem with one or more network devices to the time the problem was resolved.</p> <p><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.incidentDurationMs.</p>
cia.reasonClosed	<p>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.</p> <p><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.</p>
cia.remotemgr	<p><i>(NNMI Advanced - Global Network Management feature)</i></p> <p>Hostname or IP address of the either of the NNMI Regional Manager that is forwarding the event.</p>
cia.snmpoid	SNMP trap object identifier.
cia.timeIncidentDetectedMs	<p>The timestamp in milliseconds when NNMI first detected the problem on the network device associated with the incident.</p> <p><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),</p>

**Custom Incident Attributes Provided by NNMi, continued**

Name	Description
	NNMi does not include cia.timeIncidentDetectedMs.
cia.timeIncidentResolvedMs	<p>The time when NNMi determines the problem on the network device associated with the incident is resolved.</p> <p><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.timeIncidentResolvedMs.</p>

For network monitoring thresholds, additional custom incident attributes are provided for your use. [Click here for more information.](#)

**Custom Incident Attributes Provided for Fault Thresholds and Performance Thresholds**

Name	Description
cia.thresholdParameter	<p>The monitored attribute that is being measured. The NNMi administrator configures these thresholds.</p> <p>Possible threshold values for Nodes include:</p> <ul style="list-style-type: none"> <li>• Backplane Utilization Threshold based on the percentage of backplane usage compared to the total amount of available backplane resources.</li> <li>• Buffer Failure Rate Threshold based on the percentage of a node's buffer failures compared to the total number of attempts to create new buffers. These failures are caused by insufficient memory when the device tried to create new buffers.</li> <li>• Buffer Miss Rate Threshold based on the percentage of a Node's buffer misses compared to the total attempts at buffer access. Crossing this threshold indicates the number of available buffers are dropping below a minimum level required for successful operation.</li> <li>• Buffer Utilization Threshold based on the percentage of a Node's buffers that are currently in use, compared to the total number of available buffers.</li> <li>• CPU 5Sec Utilization</li> </ul>

**Custom Incident Attributes Provided for Fault Thresholds and Performance Thresholds, continued**

Name	Description
	<p>Threshold based on the percentage of a node's CPU usage compared to the total amount of available CPU capacity. This percentage is the average CPU utilization over the prior 5-seconds.</p> <ul style="list-style-type: none"> <li>• CPU 1Min Utilization            Threshold based on the percentage of a node's CPU usage compared to the total amount of available CPU capacity. This percentage is the average CPU utilization over the prior 1-minute.</li> <li>• CPU 5Min Utilization            Threshold based on the percentage of a node's CPU usage compared to the total amount of available CPU capacity. This percentage is the average CPU utilization over the prior 5-minutes.</li> <li>• Disk Space Utilization            Threshold based on the percentage of a node's disk space usage compared to the total amount of available disk space.</li> <li>• Memory Utilization            Threshold based on the percentage of a node's memory usage compared to the total amount of available memory.</li> <li>• Management Address ICMP Response Time            Threshold based on elapsed time (in milliseconds) for receiving a node's reply to an Internet Control Message Protocol (ICMP) echo request. The address queried is the node's Management Address attribute value. See the node's <a href="#">Node form, Basic Attributes section</a> for the currently configured address.</li> </ul> <p><i>(NNM iSPI Performance for Metrics)</i> Possible performance thresholds for Interfaces include:</p> <ul style="list-style-type: none"> <li>• FCS LAN Error Rate  <i>Local Area Network interfaces only.</i> Threshold based on the percentage of incoming frames with a bad checksum (CRC value) compared to the total number of incoming frames. Possible causes include collisions at half-duplex, a duplex mismatch, bad hardware (NIC, cable, or port), or a connected device generating frames with bad Frame Check Sequence.</li> </ul>

### Custom Incident Attributes Provided for Fault Thresholds and Performance Thresholds, continued

Name	Description
	<ul style="list-style-type: none"><li data-bbox="673 331 1391 611">• FCS WLAN Error Rate <i>Wireless Local Area Network Interfaces only.</i> Threshold based on the percentage of incoming frames with a bad checksum (CRC value) compared to the total number of incoming frames. Possible causes include wireless communication interference, bad hardware (NIC, cable or port), or a connected device generating frames with bad Frame Check Sequence.</li><li data-bbox="673 636 1391 842">• Input Discard Rate Threshold based on the percentage of the interface's discarded input packet count compared to the total number of packets received. Packets might be discarded because of a variety of issues, including receive-buffer overflows, congestion, or system specific issues.</li><li data-bbox="673 867 1391 1115">• Input Error Rate Threshold based on the percentage of the interface's input packet error count compared to the total number of packets received. What constitutes an error is system specific, but likely includes such issues as bad packet checksums, incorrect header information, and packets that are too small.</li><li data-bbox="673 1140 1391 1312">• Input Queue Drops Rate Threshold based on the percentage of the interface's dropped input packets compared to the total number of packets received. Possible causes include the input queue being full.</li><li data-bbox="673 1337 1391 1551">• Input Utilization Threshold based on the percentage of the interface's total incoming octets compared to the maximum number of octets possible (determined by the MIB being used to query <code>ifSpeed</code> of the device and whether the host system supports high-speed counters for interfaces).</li></ul> <div data-bbox="711 1570 1369 1820"><p><b>Tip:</b> Sometimes the <code>ifSpeed</code> value returned by the device's SNMP agent is not accurate and causes problems with thresholds. If your NNMi role allows, you can override the <code>ifSpeed</code> reported by the SNMP agent:</p><ol style="list-style-type: none"><li data-bbox="727 1780 1273 1820">a. Open the problem interface's Interface form.</li></ol></div>

### Custom Incident Attributes Provided for Fault Thresholds and Performance Thresholds, continued

Name	Description
	<p data-bbox="727 352 1328 491">b. Select the <a href="#">General Tab</a>. c. Locate the Input/Output Speed section. d. Change the Input Speed or Output Speed setting.</p> <ul data-bbox="675 533 1383 1415" style="list-style-type: none"><li data-bbox="675 533 1383 743">• Output Discard Rate Threshold based on the percentage of the interface's discarded output packet count compared to the total number of outgoing packets. Packets might be discarded because of a variety of issues, including transmission buffer overflows, congestion, or system specific issues.</li><li data-bbox="675 768 1383 978">• Output Error Rate Threshold based on the percentage of the interface's output packet error count compared to the total number of outgoing packets. What constitutes an error is system specific, but likely includes such issues as collisions and buffer errors.</li><li data-bbox="675 1003 1383 1184">• Output Queue Drops Rate Threshold based on the percentage of the interface's dropped output packets compared to the total number of outgoing packets. Possible causes include all buffers allocated to the interface being full.</li><li data-bbox="675 1209 1383 1415">• Output Utilization Threshold based on the percentage of the interface's total outgoing octets compared to the maximum number of octets possible (determined by the MIB being used to query <code>ifSpeed</code> of the device and whether the host system supports high-speed counters for interfaces).</li></ul> <p data-bbox="727 1457 1334 1625"><b>Tip:</b> Sometimes the <code>ifSpeed</code> value returned by the device's SNMP agent is not accurate and causes problems with thresholds. If your NNMi role allows, you can override the <code>ifSpeed</code> reported by the SNMP agent:</p> <ol data-bbox="727 1646 1328 1835" style="list-style-type: none"><li data-bbox="727 1646 1328 1677">a. Open the problem interface's Interface form.</li><li data-bbox="727 1698 1328 1730">b. Select the <a href="#">General Tab</a>.</li><li data-bbox="727 1751 1328 1782">c. Locate the Input/Output Speed section.</li><li data-bbox="727 1803 1328 1835">d. Change the Input Speed or Output Speed setting.</li></ol>

### Custom Incident Attributes Provided for Fault Thresholds and Performance Thresholds, continued

Name	Description
cia.thresholdLowerBound	The configured value for the low threshold.
cia.thresholdUpperBound	The configured value for the high threshold.
cia.thresholdPreviousValue	Results from the previous Fault Polling Interval or Performance Polling Interval. For example, the performance threshold results for Interface Input Error Rate might change from <b>Nominal</b> to <b>High</b> , based on a change in the thresholdMeasuredValue. See <a href="#">Interface Form</a> for a complete list of possible values.
cia.thresholdCurrentValue	Results from the most recent Fault Polling Interval or Performance Polling Interval. For example, <b>High</b> . See <a href="#">Interface Form</a> for a complete list of possible values.
cia.thresholdMeasuredValue	The most recent measurement for the threshold monitored for violations. This measurement is the average of all measurements taken during the last polling interval (determined by the NNMi State Poller).
cia.thresholdMeasurementTime	The time at which the threshold was reached. For example, if a threshold for the Input Error Rate is 6.0, and the thresholdMeasuredValue is 6.0, the time at which the thresholdMeasuredValue become equal to 6.0 is stored in this custom incident attribute. The time appears in ISO 8601 format.

#### Related Topics

"Custom Incident Attribute Form" on page 321

## Incident Form: Diagnostics Tab (*NNM iSPI NET*)

The "Incident Form" on page 311 provides details for troubleshooting purposes.

For information about each tab:

#### Diagnostics Table

Attribute	Description
List of Diagnostics	<p>The history of all the HP Network Node Manager iSPI Network Engineering Toolset Software 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.</p> <p>To generate a new instance of these Diagnostics reports, click <b>Actions</b> → <b>Run Diagnostics (iSPI NET only)</b>.</p>



### Diagnostics Table, continued

Attribute	Description
	<p><b>Tip:</b> You can right-click any object in a table or map view to access the <b>Actions</b> menu.</p> <p>Double-click the row representing a Diagnostic report. NNMi displays all details about the selected report. See "Incident Diagnostic Results Form (Flow Run Result) (NNM iSPI NET)" below.</p>

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

HP Network Node Manager iSPI Network Engineering Toolset Software automatically prepares diagnostic reports when certain incidents are generated and when using **Actions** → **Run Diagnostics (iSPI NET only)**. This form shows details about the currently selected diagnostic report instance.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

**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 the previous page for more information:

### Diagnostic Results Details

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 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 timeout error. The timeout limit for submitting a Diagnostic is one hour. The timeout limit for running a Diagnostic is four hours.</p> <p>Example error conditions include the following:</p>

### Diagnostic Results Details, continued

Attribute	Description
	<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>NNM iSPI NET uses this text string to display the selected instance of the diagnostics report in a browser window.</p> <p>Click this link to open the actual report.</p> <div style="background-color: #f0f0f0; padding: 5px;"> <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> </div>
Lifecycle State	<p>Incident <a href="#">Lifecycle State</a> of the target Incident.</p> <p>If the incident's Lifecycle State matches the value specified here, the Diagnostic runs.</p> <p>The Diagnostic automatically runs on each applicable Source Node in the specified Node Group if the incident has the Lifecycle State currently configured in this attribute of the Diagnostic (Flow Definition - set of automated commands).</p>
Last Update Time	<p>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.</p>

## Incident Form: Registration Tab

The "Incident Form" on page 311 provides details for troubleshooting purposes.

**For information about each tab:**

### Registration Attributes

Attribute	Description
Created	Date and time the selected object instance was created. NNMI 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. NNMI uses the locale of the client and the date and time from the NNMI management server.

### Object Identifiers Attributes

Attribute	Description
ID	The Unique Object Identifier, which is unique within the NNMi database.
UUID	The Universally Unique Object Identifier, which is unique across all databases.

## 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.

**Note:** If a node is deleted, only an NNMi administrator can view the incidents associated with that node.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

### Tasks Related to Assigning Incidents

Task	How	Required Minimum NNMi User Role
Own an incident	Select an incident and use <b>Actions</b> → <b>Assign</b> → <b>Own Incident</b> . See " <a href="#">Own Incidents</a> " below for more information.	Level 1 Operator (with less access privileges than Level 2 Operators)
Assign an incident to someone else	There are two ways to assign an incident to someone else (see " <a href="#">Assign Incidents</a> " on the next page 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</b> → <b>Assign Incident</b>.</li><li>From an Incident form, use <b>Actions</b> → <b>Assign</b> → <b>Assign Incident</b>.</li></ul>	Level 1 Operator
Un-assign an incident	Select an incident and use <b>Actions</b> → <b>Assign</b> → <b>Unassign Incident</b> . See " <a href="#">Unassign Incidents</a> " on page 333 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:**

1. Navigate to the incident view of interest.
  - a. From the workspace navigation panel, select the **Incident Management** or **Incident Browsing** workspace.
  - b. Select the incident view of interest; for example **Unassigned Open Key Incidents**.
2. Press CTRL-Click and select each row that represents an incident you want to own.
3. Select **Actions** → **Assign** → **Own Incident**.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

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 342 for more information.

## Assign Incidents

If you are an NNMi user with a Level 1 Operator (with less access privileges than Level 2 Operators), 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](#).

**Note:** Make sure an operator can access the incidents that are assigned to him or her. See "[Node and Incident Access](#)" on page 19 for more information.

### 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. Select the row representing the incident you want to assign.
2. Select **Actions** → **Assign** → **Assign Incident**.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

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 345 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. Press CTRL-Click and select each row that represents an incident you want to assign.
3. Select **Actions** → **Assign** → **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 345 for more information.

## Unassign Incidents

If you are an NNMI user with a user role of Level 1 Operator (with less access privileges than Level 2 Operators), 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. Select the row representing the incident you want to unassign.
2. Select **Actions** → **Assign** → **Unassign Incident**.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

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 345 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. Press CTRL-Click and select each row that represents an incident you want to unassign.
  3. Select **Actions** → **Assign** → **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 345 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.

**Note:** If a node is deleted, only an NNMi administrator can view the incidents associated with that node.

### 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, spaces, and special characters (~ ! @ # \$ % ^ & \* ( ) \_ + -) are permitted.
4. If you need more space to type in your information, click the **Notes** label, and type the information into the window that appears.
5. 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 State](#) information up-to-date. See "[Track an Incident's Progress](#)" on page 336 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.
- 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 the [Lifecycle State](#) information for the Incident form for more information). See also "[Track an Incident's Progress](#)" on the next page.

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.
- 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.


## Track an Incident's Progress

NNMi provides the **Lifecycle State** attribute to help you track an incident's progress. Your network administrator might have additional or different guidelines for their use.

Possible Lifecycle State values are as follows:

-  **Registered** – Indicates that an incident arrived in the queue stored in the NNMi database.
-  **In Progress** – State selected by someone on your team to indicate that they are taking responsibility for investigating the problem.
-  **Completed** – State selected by someone on your team to indicate completion of the incident investigation and implementation of a solution.
-  **Closed** – Indicates that NNMi determined 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.

**Note:** NNMi does not automatically Close incidents whose Correlation Nature is **Info**. These incidents are meant to provide information regarding changes in your network that might be of interest. You will need to Close these incidents if you do not want them to remain in your incident queue. See "[Incident Form: General Tab](#)" on page 314 for more information about Correlation Nature

-  **Dampened** – Indicates that, within the configured *acceptable time period*, NNMi determined the problem reported by this Incident is no longer a problem. NNMi does not submit the incident to the queue until after the time period (configured by the NNMi administrator).

In some cases, NNMi updates an incident's Lifecycle State for you. See "[About the Incident Lifecycle](#)" on the previous page for more information about **Lifecycle State**.

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** → **Change Lifecycle** menu or a form.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

### 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. Select the row representing the incident that has a Lifecycle State you want to change.
3. From the main menu toolbar, select **Actions** → **Change Lifecycle** 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**.

3. 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. In any table of incidents, select the incident of interest by selecting the appropriate row.
2. Select **Actions** → **Maps** → **Node Group Map** in the main toolbar.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

The map displays based on the source node of the selected incident:

- 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 the incident is associated with an Island Node Group, NNMI displays the associated Island Node Group map. See "[Island Node Group Map](#)" on the next page for more information.
- If the Source Node is not a member of any Node Group, NNMI informs you that no Node Group map is available.

**Note:** Your NNMI administrator sets some of management mode attribute values. The current values of the management mode attributes determine whether NNMI discovers and monitors a node, interface, or address. 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 261](#)

["Display the Layer 3 Neighbor View" on page 263](#)

["Path Between Two Nodes that Have IPv4 Addresses" on page 265](#)

["Node Group Overview Map" on page 257](#)

["Routers Map" on page 260](#)

["Switches Map" on page 260](#)

["Networking Infrastructure Devices Map" on page 259](#)

["Display a Line Graph from an Incident \(Custom Poller Only\)" on page 306](#)

## Island Node Group Map

An Island Group is a group of fully-connected nodes discovered by NNMi, and NNMi determines this group is 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 that have a Source Object that 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. Select the row representing an Island Node Group incident that has the map you want to display.
3. Select **Actions** → **Maps** → **Node Group Map**.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

### Related Topics

[Node Group Map Objects](#)

## Apply an Action to an Incident Source Node or Source Object

If you are using incident views to monitor your network, you might want to apply an action from the Actions menu to the incident Source Node or Source Object to determine more information. NNMi enables you to access the same actions that are available for node, interface, and IP address objects.

**Note:** Only the Actions that apply to either the incident's Source Node or Source Object are available. If the Action does not apply to either the Source Node or Source Object, the color of that Action turns from black to gray to indicate it is unavailable.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

**To access an action from an incident view:**

1. Navigate to the incident view of interest (for example, **Incident Browsing** workspace, **Root Cause Incidents** view).
2. Select the row representing the incident of interest.  
**Note:** Select only one incident.
3. From the Actions menu in the main toolbar, select one of the following menu options:
  - Node Actions
  - Interface Actions
  - IP Address Actions
4. Select an action that is valid for either the incident Source Node or Source Object. See [Using Actions to Perform Tasks](#) for information about the actions available for each object type. Also see ["Investigate and Diagnose Problems"](#) on page 355.

NNMi performs the selected action on whichever of the following is the valid object for the action selected:

- Incident's Source Node
- Incident's Source Object

**To access an action from an incident form:**

1. Navigate to the incident view of interest (for example, **Incident Browsing** workspace, **Root Cause Incidents** view).
2. Double-click the row representing the incident from which you want to select an action.
3. From the Actions menu in the main toolbar, select one of the following:
  - Node Actions
  - Interface Actions
  - IP Address Actions
4. Select an action that is valid for either the incident Source Node or Source Object. See [Using Actions to Perform Tasks](#) for information about the actions available for each object type. Also see ["Investigate and Diagnose Problems"](#) on page 355.

NNMi performs the selected action on whichever of the following is the valid object for the action selected:

- Incident's Source Node
- Incident's Source Object

**Related Topics**

["Display a Line Graph from an Incident \(Custom Poller Only\)"](#) on page 306

## Monitor Incidents in a Global Network Management Environment (*NNMi Advanced*)

The NNMi Global Network Management feature enables multiple NNMi management servers to work together while managing different geographic areas of your network. Each NNMi management server discovers and monitors a portion of the network.

Specific NNMi management servers can be designated as *Global Managers* and display the combined Node object data. However, each Regional Manager maintains responsibility for management of Nodes that were forwarded to a Global Manager. The Global Manager generates and maintains an independent set of Incidents related to those Nodes. The Incidents on the Global Manager are generated within the context of the combined topology and using the Incident configuration settings on the Global Management server.

Regional Manager administrators can intentionally forward copies of two types of incidents to the Global Manager:

- SNMP Trap Incidents
- Remote NNM 6.x/7.x Event Incidents

On the Global Manager, the **Custom Incident Attribute** tab on the Incident form identifies if the SNMP trap or NNM 6.x/7.x Event was forwarded and from which Regional Manager.

**From any Incident view, to determine the server or servers that forwarded the incident:**

1. From the workspace navigation panel, select a workspace containing a view of the incidents of interest (for example, **Incident Management** workspace).
2. Select a view that contains the specific incident (for example **Open Key Incidents** view).
3. Double-click the row representing an incident. The Incident Form displays all details about the selected incident.
4. Navigate to the **Custom Attributes** tab.
5. In the **Name** column of table view, look for the following value: `cia.remotemgr`.
  - If `cia.remotemgr` is not listed, this means the incident was not forwarded from a NNM 6.x/7.x management station or Regional Manager.
  - If `cia.remotemgr` appears in the list of Custom Attributes, NNMi displays the hostname of the NNMi Regional Manager or NNM 6.x/7.x management station in the corresponding **Value** column.

**Note:** If the trap or event has been forwarded through multiple servers, `cia.remotemgr` includes the hostname or IP address of each forwarding server, separated by commas. The list of servers provided in `cia.remotemgr` starts with the server that generated the original SNMP trap, 6.x/7.x event, or management event incident.

## 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 views for listing incident

information:

**Note:** NNMi generates informational incidents that do not appear by default in incident views.

These incidents are advisory and have a Correlation Nature of **Info**. To view these incidents, create a filter for the **All Incidents** view using the Correlation Nature column and select the value **Info** from the enumerated list of values. See [Filter a Table View](#) for more information about filtering table views.

- ["Open Key Incidents View" on page 344](#)
- ["Unassigned Open Key Incidents View" on page 345](#)
- ["My Open Incidents View" on the next page](#)
- ["Closed Key Incidents View" on page 346](#)
- ["Open Root Cause Incidents View"](#)
- ["Service Impact Incidents View" on page 349](#)
- ["All Incidents View" on page 350](#)
- ["Custom Open Incidents View" on page 350](#)
- ["Custom Incidents View" on page 351](#)
- ["NNM 6.x/7.x Events View " on page 352](#)
- ["SNMP Traps View" on page 353](#)

The most useful views for proactively monitoring your network for problems are the [Key Incident](#)<sup>1</sup> views (see ["Key Incident Views" on page 343](#)). 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 ["NNM 6.x/7.x Events View " on page 352](#) 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

---

<sup>1</sup>Incidents with both: (1) Severity = other than Normal. (2) Correlation Nature = equal to Root Cause, Service Impact, Stream Correlation, Rate Stream Correlation, Info, or None.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

Other useful tasks from the incident view, include the following:

- "Display a Map from an Incident" on page 337
- "Node Form" on page 50

**Related Topics:**

[About Workspaces](#)




[About the NNMi Console](#)

## My Open Incidents View

**Tip:** See "Incident Form" on page 311 for more details about the incident attributes that appear in this view's column headings.

This view is useful for identifying the incidents for which you are responsible.

The **My Open Incidents** view displays all of the open incidents that meet this criterion:

- Assigned to you.
- Lifecycle state matching any of the following:
  -  **Registered**
  -  **In Progress**
  -  **Completed**

As with all incident views, you can filter this view by time period. The default time period is **Last Week**.

For each incident displayed, you can view its severity, its priority, its lifecycle state (see the [Lifecycle State](#) information for the Incident form for more information), 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, **NNMi**, **NNM 6.x/7.x**, or **SNMP Trap**), its Correlation Nature (for example, **Symptom** or **Root Cause**), the message used to describe the incident, and any related notes.

Note the following:

- If your NNMi Administrator defines at least one Tenant in addition to Default Tenant (provided by NNMi), the incident view displays the Tenant to which the Source Node belongs. If you are an NNMi administrator, see [Configure Tenants](#) for more information about Tenants.
- Global Network Management *only*. The Regional Manager **Name** value that is associated with the Source Node's NNMi Management Server appears in the incident view on the Global Manager console. If the incident's Source Node no longer exists, the Management Server value is blank.

See "Monitoring Incidents for Problems" on page 309 for more information about ways to use incident views.

## Key Incident Views

**Tip:** See "Incident Form" on page 311 for more details about the incident attributes that appear in a key incident view's column headings.

The **Key Incident**<sup>1</sup> views are useful for identifying incidents that are most important to the network Operator and that often require more immediate action.

The Key Incident views display incidents that meet the following criterion:

- Severity is *other than* Normal.
- Correlation Nature is any of the following:

Incident Correlation Nature	Description
Root Cause	Indicates the incident that reports the root cause of a problem.
Service Impact	<p><i>Used in NNMi 8.xx only.</i> 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 HP Network Node Manager i Software Smart Plug-ins (iSPIs). See "Help for Administrators" for more information about NNM iSPIs.</p>
Stream Correlation	<p><i>Used in NNMi 8.xx only.</i> 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.</p>
Rate Stream Correlation	Indicates the incident tracks incident patterns <i>based on the number of incident reoccurrences within a specified time period.</i> After the count within the specified time period is reached, NNMi emits a Rate Correlation incident and continues to update the Correlation Notes with the number of occurrences within that rate.
Info	This Correlation Nature is meant to be informational.
None	Indicates there is no incident correlation for this incident.

---

<sup>1</sup>Incidents with both: (1) Severity = other than Normal. (2) Correlation Nature = equal to Root Cause, Service Impact, Stream Correlation, Rate Stream Correlation, Info, or None.

Some Key Incident views are filtered according to lifecycle state values (see the [Lifecycle State](#) information for the Incident form for more information), which can be set by the user.

NNMi provides the following Key Incident views filtered to display lifecycle state values of **Registered**, **In Progress**, or **Completed**:

- "Open Key Incidents View" below

NNMi provides the following Key Incident view filtered to display lifecycle state value of **Closed**:

- "Open Key Incidents View" below "Closed Key Incidents View" on page 346

NNMi provides the following Key Incident view filtered to display (1) lifecycle state values of **Registered**, **In Progress**, and **Completed** plus (2) assigned to value equal to **none**:

- "Unassigned Open Key Incidents View" on the next page

### Related Topics

[Use Table Views](#)

["Organize Your Incidents" on page 311](#)

["Monitoring Incidents for Problems" on page 309](#)

["Display a Map from an Incident" on page 337](#)

## Open Key Incidents View

**Tip:** See "Incident Form" on page 311 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 any **Key Incident**<sup>1</sup> that has a Lifecycle State value that indicates 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.

**Note:** Only incidents that have a Severity other than Normal are included in **Key Incident**<sup>2</sup> views.

For each incident displayed, you can view its severity, its priority, its lifecycle state (see the [Lifecycle State](#) information for the Incident form for more information), 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, **NNMi**, **NNM 6.x/7.x**, or **SNMP Trap**), its **Correlation Nature** (for example, **Root Cause**), the message used to describe the incident, and any related notes.

Note the following:

---

<sup>1</sup>Incidents with both: (1) Severity = other than Normal. (2) Correlation Nature = equal to Root Cause, Service Impact, Stream Correlation, Rate Stream Correlation, Info, or None.

<sup>2</sup>Incidents with both: (1) Severity = other than Normal. (2) Correlation Nature = equal to Root Cause, Service Impact, Stream Correlation, Rate Stream Correlation, Info, or None.



- If your NNMi Administrator defines at least one Tenant in addition to Default Tenant (provided by NNMi), the incident view displays the Tenant to which the Source Node belongs. If you are an NNMi administrator, see [Configure Tenants](#) for more information about Tenants.
- Global Network Management *only*. The Regional Manager **Name** value that is associated with the Source Node's NNMi Management Server appears in the incident view on the Global Manager console. If the incident's Source Node no longer exists, the Management Server value is blank.

See "[Monitoring Incidents for Problems](#)" on page 309 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 311](#)

["Monitoring Incidents for Problems" on page 309](#)

["Display a Map from an Incident" on page 337](#)

["Key Incident Views" on page 343](#)

["Unassigned Open Key Incidents View" below](#)

["Closed Key Incidents View" on the next page](#)

## Unassigned Open Key Incidents View

**Tip:** See "[Incident Form](#)" on page 311 for more details about the incident attributes that appear in this view's column headings.

The **Unassigned Open Key Incident** view displays any [Key Incident](#)<sup>1</sup> that is open and unassigned. 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.

**Note:** Only incidents that have a Severity that is other than Normal are included in Key Incident views.

For each incident displayed, you can view its severity, its priority, its lifecycle state (see the [Lifecycle State](#) information for the Incident form for more information), 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, **NNMi**, **NNM 6.x/7.x**, or **SNMP Trap**), its Correlation Nature (for example, **Root Cause**), the message used to describe the incident, and any related notes.

---

<sup>1</sup>Incidents with both: (1) Severity = other than Normal. (2) Correlation Nature = equal to Root Cause, Service Impact, Stream Correlation, Rate Stream Correlation, Info, or None.

Note the following:

- If your NNMi Administrator defines at least one Tenant in addition to Default Tenant (provided by NNMi), the incident view displays the Tenant to which the Source Node belongs. If you are an NNMi administrator, see [Configure Tenants](#) for more information about Tenants.
- Global Network Management *only*. The Regional Manager **Name** value that is associated with the Source Node's NNMi Management Server appears in the incident view on the Global Manager console. If the incident's Source Node no longer exists, the Management Server value is blank.

See "[Monitoring Incidents for Problems](#)" on page 309 for more information about ways to use incident views.

### Related Topics

[Use Table Views](#)

["Organize Your Incidents" on page 311](#)

["Monitoring Incidents for Problems" on page 309](#)

["Display a Map from an Incident" on page 337](#)


["Key Incident Views" on page 343](#)

["Open Key Incidents View" on page 344](#)

["Closed Key Incidents View" below](#)

## Closed Key Incidents View

**Tip:** See "[Incident Form](#)" on page 311 for more details about the incident attributes that appear in this view's column headings.

The **Closed Key Incidents** view displays any [Key Incident](#)<sup>1</sup> with a Life Cycle state of  **Closed** (see the [Lifecycle State](#) information for the Incident form for more information). 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 that have a Correlation Nature of **Info**. The **Info** Correlation Nature is meant to be informational.

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 a Last Occurrence Time 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.

**Note:** Only incidents that have a Severity that is other than Normal are included in [Key Incident](#)<sup>2</sup> views.

---

<sup>1</sup>Incidents with both: (1) Severity = other than Normal. (2) Correlation Nature = equal to Root Cause, Service Impact, Stream Correlation, Rate Stream Correlation, Info, or None.

<sup>2</sup>Incidents with both: (1) Severity = other than Normal. (2) Correlation Nature = equal to Root Cause, Service Impact, Stream Correlation, Rate Stream Correlation, Info, or None.

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, **NNMi**, **NNM 6.x/7.x**, or **SNMP Trap**), the message used to describe the incident, and any related notes.

Note the following:

- If your NNMi Administrator defines at least one Tenant in addition to Default Tenant (provided by NNMi), the incident view displays the Tenant to which the Source Node belongs. If you are an NNMi administrator, see [Configure Tenants](#) for more information about Tenants.
- Global Network Management *only*. The Regional Manager **Name** value that is associated with the Source Node's NNMi Management Server appears in the incident view on the Global Manager console. If the incident's Source Node no longer exists, the Management Server value is blank.

See ["Monitoring Incidents for Problems"](#) on page 309 for more information about ways to use incident views.

**Related Topics:**

[Use Table Views](#)

["Organize Your Incidents"](#) on page 311

["Monitoring Incidents for Problems"](#) on page 309

["Display a Map from an Incident"](#) on page 337

["Key Incident Views"](#) on page 343

["Open Key Incidents View"](#) on page 344

["Unassigned Open Key Incidents View"](#) on page 345

## Root Cause Incidents

**Tip:** See ["IP Address Form"](#) on page 132 ["Incident Form"](#) on page 311 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. For example, NNMi notifies you if it encounters any of the following situations:

- ["Node Down"](#) on page 404
- ["Interface Down"](#) on page 401
- ["Address Not Responding"](#) on page 388

NNMi provides the ["Open Root Cause Incidents View"](#) on the next page

**When using root cause incident views, note the following:**

- Your administrator might 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**.

See "[Monitoring Incidents for Problems](#)" on page 309 for more information about ways to use incident views.

**Related Topics:**

[Use Table Views](#)

["Organize Your Incidents" on page 311](#)

["Monitoring Incidents for Problems" on page 309](#)

["Display a Map from an Incident" on page 337](#)

## Open Root Cause Incidents View

**Tip:** See "[Incident Form](#)" on page 311 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 that have a Lifecycle State other than 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.

You might also choose to narrow your focus by filtering this information according to one or more attribute values, such as all root cause incidents that have a Status of Critical, or all root cause incidents that have the description **Node Down**.

For each incident displayed, you can view its severity, its priority, its lifecycle state (see the [Lifecycle State](#) information for the Incident form for more information), 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, **NNMi**, **NNM 6.x/7.x**, or **SNMP Trap**), the message used to describe the incident, and any related notes.

Note the following:

- If your NNMi Administrator defines at least one Tenant in addition to Default Tenant (provided by NNMi), the incident view displays the Tenant to which the Source Node belongs. If you are an NNMi administrator, see [Configure Tenants](#) for more information about Tenants.
- Global Network Management *only*. The Regional Manager **Name** value that is associated with the Source Node's NNMi Management Server appears in the incident view on the Global Manager console. If the incident's Source Node no longer exists, the Management Server value is blank.

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.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

**Related Topics:**

[Use Table Views](#)

["Organize Your Incidents" on page 311](#)

["Monitoring Incidents for Problems" on page 309](#)

["Display a Map from an Incident" on page 337](#)

["Unassigned Open Key Incidents View" on page 345](#)

["Closed Key Incidents View" on page 346](#)

## Service Impact Incidents View

**Tip:** See ["Incident Form" on page 311](#) 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 that have a Correlation Nature of **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 affect a Router Redundancy Group that is part of an HSRP service. This view is useful to identify a service that is affected.

**Note:** The **Service Impact** Correlation Nature is available for use by HP Network Node Manager i Software Smart Plug-ins (iSPIs). See ["Help for Administrators"](#) for more information about NNM iSPIs.

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 (see the [Lifecycle State](#) information for the Incident form for more information), 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.

Note the following:

- If your NNMi Administrator defines at least one Tenant in addition to Default Tenant (provided by NNMi), the incident view displays the Tenant to which the Source Node belongs. If you are an NNMi administrator, see [Configure Tenants](#) for more information about Tenants.
- Global Network Management *only*. The Regional Manager **Name** value that is associated with the Source Node's NNMi Management Server appears in the incident view on the Global Manager console. If the incident's Source Node no longer exists, the Management Server value is blank.

See ["Monitoring Incidents for Problems" on page 309](#) for more information about ways to use incident views.

## All Incidents View

**Tip:** See "Incident Form" on page 311 for more details about the incident attributes that appear in this view's column headings.

The **All Incidents** view is useful for viewing all of the incidents generated by NNMi within the specified time period. This view is useful to identify both Open and Closed incidents. 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 occurred within the last 24 hours.

For each incident displayed, you can view its severity, its priority, its lifecycle state (see the [Lifecycle State](#) information for the Incident form for more information), 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, **NNMi**, **NNM 6.x/7.x**, or **SNMP Trap**), its Correlation Nature (for example, **Symptom** or **Root Cause**), the message used to describe the incident, and any related notes.

Note the following:

- If your NNMi Administrator defines at least one Tenant in addition to Default Tenant (provided by NNMi), the incident view displays the Tenant to which the Source Node belongs. If you are an NNMi administrator, see [Configure Tenants](#) for more information about Tenants.
- Global Network Management *only*. The Regional Manager **Name** value that is associated with the Source Node's NNMi Management Server appears in the incident view on the Global Manager console. If the incident's Source Node no longer exists, the Management Server value is blank.

See "Monitoring Incidents for Problems" on page 309 for more information about ways to use incident views.

## Custom Open Incidents View

**Tip:** See "Incident Form" on page 311 for more details about the incident attributes that appear in this view's column headings.

The **Custom Open Incidents** view lets you choose the columns of incident information for all Open incidents, 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 (see the [Lifecycle State](#) information for the Incident form for more information), 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, **NNMi**, **NNM 6.x/7.x**, 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.

Note the following:

- If your NNMi Administrator defines at least one Tenant in addition to Default Tenant (provided by NNMi), the incident view displays the Tenant to which the Source Node belongs. If you are an NNMi administrator, see [Configure Tenants](#) for more information about Tenants.
- Global Network Management *only*. The Regional Manager **Name** value that is associated with the Source Node's NNMi Management Server appears in the incident view on the Global Manager console. If the incident's Source Node no longer exists, the Management Server value is blank.

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

See ["Monitoring Incidents for Problems"](#) on page 309 for more information about ways to use incident views.

See ["Incident Form"](#) on page 311 for more information about incident attributes.

**Related Topics:**

[Use Table Views](#)

["Organize Your Incidents"](#) on page 311

["Display a Map from an Incident"](#) on page 337

## Custom Incidents View

**Tip:** See ["Incident Form"](#) on page 311 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 (see the [Lifecycle State](#) information for the Incident form for more information), 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, **NNMi**, **NNM 6.x/7.x**, 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.

Note the following:

- If your NNMi Administrator defines at least one Tenant in addition to Default Tenant (provided by NNMi), the incident view displays the Tenant to which the Source Node belongs. If you are an NNMi administrator, see [Configure Tenants](#) for more information about Tenants.
- Global Network Management *only*. The Regional Manager **Name** value that is associated with the Source Node's NNMi Management Server appears in the incident view on the Global Manager console. If the incident's Source Node no longer exists, the Management Server value is blank.

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

See ["Monitoring Incidents for Problems"](#) on page 309 for more information about ways to use incident views.

See ["Incident Form"](#) on page 311 for more information about incident attributes.

**Related Topics:**

[Use Table Views](#)

["Organize Your Incidents"](#) on page 311

["Display a Map from an Incident"](#) on page 337

## NNM 6.x/7.x Events View

**Tip:** See ["Incident Form"](#) on page 311 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**

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

See ["Accessing NNM 6.x and 7.x Features"](#) on page 25 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 (see the [Lifecycle State](#) information for the Incident form for more information), the date and time the incident last occurred, the name of its source node, 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.

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.

## Syslog Messages View (HP ArcSight)

**Tip:** See "Incident Form" on page 311 for more details about the incident attributes that appear in this view's column headings.

The HP NNMi–ArcSight integration adds syslog message information to NNMi, so that you can view these syslog messages and investigate potential problems. After the ArcSight integration is enabled, NNMi receives `ArcSightEvent` traps that contain syslog message data. NNMi then maps this syslog information to a Syslog Message incident configuration and treats it as a syslog message in NNMi. The **Syslog Messages** view in the **Incident Browsing** workspace displays these incidents.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

For each incident displayed, you can view its Severity, its Lifecycle State (see the [Lifecycle State](#) information for the Incident form for more information), the date and time the incident last occurred, the name of its Source Node and 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.

Note the following:

- If your NNMi Administrator defines at least one Tenant in addition to Default Tenant (provided by NNMi), the incident view displays the Tenant to which the Source Node belongs. If you are an NNMi administrator, see [Configure Tenants](#) for more information about Tenants.
- Global Network Management *only*. The Regional Manager **Name** value that is associated with the Source Node's NNMi Management Server appears in the incident view on the Global Manager console. If the incident's Source Node no longer exists, the Management Server value is blank.

As with all incident views, you can filter this view by time period. The default time period is **Last Hour**.

## SNMP Traps View

**Tip:** See "Incident Form" on page 311 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 the most recent incidents.

For each incident displayed, you can view its severity, its lifecycle state (see the [Lifecycle State](#) information for the Incident form for more information), 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.

Note the following:

- If your NNMi Administrator defines at least one Tenant in addition to Default Tenant (provided by NNMi), the incident view displays the Tenant to which the Source Node belongs. If you are an NNMi administrator, see [Configure Tenants](#) for more information about Tenants.
- Global Network Management *only*. The Regional Manager **Name** value that is associated with the Source Node's NNMi Management Server appears in the incident view on the Global Manager console. If the incident's Source Node no longer exists, the Management Server value is blank.

# Chapter 9

---

## Investigate and Diagnose Problems

NNMi offers several ways for you to investigate and diagnose network problems.

- 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 387 for more information.

For information about a specific Root Cause Incident message:



- Start by accessing the available information for the Source Object and Source Node for the incident. To access all known information about the Source Object, access the incident's Source Object form. NNMi monitors the following object types:
  - Node and its Node Components, such as fans
  - Interface
  - IP Address
  - Cards
  - SNMP Agents
  - Node Groups
  - Card Redundancy Groups
  - Router Redundancy Groups

- Select an incident. Then, select **Actions** → **Source Object**. NNMi displays the form for the object associated with the incident.

A wealth of information about that object is available.

- The object's form is displayed in the top half of the display window. Use the **Conclusions** tab to display a history of any problems that led to the object's current Status.
- The Analysis Pane is displayed in the bottom half of the display window. It provides a quick summary of available information. For example, the **Details** tab also lists the available Conclusions.

To explore the information about the object, use the browse buttons:

-  to display a list of all available tabs. Select any tab name from the list to display that tab.
-  to display the next subset of tabs (depending on the current width of your NNMi window).

You will find the object's **State**, **Status** (No Status, Normal, Warning, Minor, Major, Critical, Disabled, or Unknown), **Conclusions**, and any related incidents.

- If the Source Object is not a node, you can access the form for the node on which the object is

hosted by selecting **Open** using the  Lookup icon from the **Hosted on Node** attribute.

Once again, information about the State, Status, and Conclusions can assist you with identifying the problem.

- 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 359
  - "View the Monitoring Settings Report" on page 360
  - "Verify Current Status of a Device" on page 385
- The Actions menu also provides an easy way to use troubleshooting commands to diagnose node connectivity and access problems:
  - "Display End Nodes Attached to a Switch" on page 452
  - "Test Node Access (Ping)" on page 454
  - "Find the Route (traceroute)" on page 455
  - "Establish Contact with a Node (Telnet or Secure Shell)" on page 456
  - "Check Status Details for a Node Group" on page 458
  - "Accessing NNM 6.x and 7.x Features" on page 25

**Note:** You can also access Line Graphs from the **Actions** menu to investigate a problem. See "Monitor with Line Graphs" on page 294 for more information.

- Use **Tools** → **SNMP MIB Browser** or select **Actions** → **MIB Information** → **Browse MIB** from a Node or Incident form to view MIB Information for a node. See "View MIB Information for a Node (MIB Browser)" on page 362 for more information.
- If you have NNMI role permits, you can use **Actions** → **Open Incident Configuration** to access more information about the incident including its Description, which includes reasons why the incident is generated.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

- 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 447
  - "Find the Attached Switch Port" on page 449
  - "Checking the Status of NNMI" on page 460


## Use the Analysis Pane

To begin diagnosing a problem, you might want to gather current information about the object.


The Analysis Pane displays related details about the selected object. NNMi performs the appropriate analysis on the selected object to determine the most important information to display. Any hyperlink within the Analysis Pane displays more information about the selected detail.

Examples of the types of related information includes details about an incident's Source Node and Source Object or information about a node's Interfaces and IP Addresses. See the [Examples of Possible Analysis Pane Information](#) table for more examples of the types of analysis data displayed.

#### To access the Analysis Pane from a table view:

1. Select the workspace of interest (for example,  **Inventory**).
2. Select the view that contains the object of interest (for example, the **Nodes** view).
3. Select the row that contains the object of interest.
4. NNMi displays detailed information at the bottom of the view in the Analysis Pane.


#### To access the Analysis Pane in a map view:


1. Select the workspace of interest (for example,  **Topology Maps**).
2. Select a map view (for example, select **Routers**).

**Note:** If the map requires a starting node before it opens, enter the name or IP Address for the starting node you want to use.

3. Click the map object of interest.
4. NNMi displays detailed information at the bottom of the view in the Analysis Pane.

#### To access the Analysis Pane in a form:

- Click the form's toolbar  Show Analysis icon to display information about the current form's top-level object in the Analysis Pane.

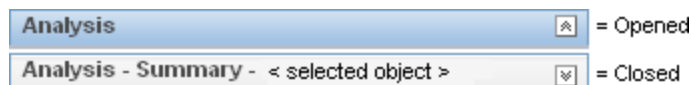
**Note:**  Show Analysis always displays the top-level object's information.

- Click a row in a table on one of the form's tabs to display detailed information about the selected object in the Analysis Pane.


NNMi displays detailed information at the bottom of the form in the Analysis Pane. See [Working with Objects](#) for more information about forms.


Note the following:

- Look for one of the following at the bottom of the display area:



Open the Analysis Pane if necessary by clicking the  expand button.

- Place your mouse cursor over the title bar to display the  symbol, then resize as necessary.
- The Analysis Pane remains blank until an object is selected.

- If you select multiple objects or clear a selection, NNMI retains the Analysis Pane's contents.
- If you change views, NNMI clears the Analysis Pane.
- Click any  Refresh icon in the Analysis Pane to update a subset of displayed information.
- NNMI automatically refreshes the entire Analysis Pane's contents when you save a form.
- The Gauges tab shows real-time SNMP gauges to display State Poller and Custom Poller SNMP data.
  - These gauges are displayed for Nodes, Interfaces, Custom Node Collections, and for Node Components of type CPU, Memory, Buffers, or Backplane.
  - NNMI displays a gauge for each significant MIB Object Identifier (OID) that the node or interface supports, up to the default maximum of 24.

**Tip:** If you are an NNMI administrator, for information about using the `nms-ui.properties` file to change this default, see the "NNMI Console" chapter in the *HP Network Node Manager i Software Deployment Reference*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>.

- Each gauge displays the current OID value, using the default refresh rate of 15 seconds. (If you are an NNMI administrator, for information about using the `nms-ui.properties` file to change this default, see the "NNMI Console" chapter of the *HP Network Node Manager i Software Deployment Reference*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>.)
- The value range displayed indicates the OID minimum and maximum values that NNMI has encountered.
- For any gauge that tracks percentage values, NNMI uses a red line to indicate where the OID value is near 100 percent.
- There is not a one-to-one match between the OIDs used to analyze monitoring thresholds and those displayed in the Analysis Pane. For example, the Analysis Pane might display a **Cisco Memory Pool** OID value that does not match the value used to calculate whether the **Memory Utilization** Monitored Attribute threshold is reached or exceeded. This is because some threshold metrics require more complex calculations than a single OID allows.

**Tip:** If a gauge label appears to be a duplicate value, mouse over the label to view the more complete tooltip name that appears. (If you are an NNMI administrator, to change the gauge title from the NNMI component name to the SNMP MIB variable name, see the "Maintaining NNMI" chapter of the *HP Network Node Manager i Software Deployment Reference*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>.)

- To launch an SNMP Line Graph for the selected metric, click the icon that appears at the bottom of each gauge.
- To select and copy the tooltip information, double-click the gauge. NNMI opens a text window that enables you to select and copy the tooltip information.

**Tip:** Some views are also accessible from the console's Actions menu. See [Using Actions to Perform Tasks](#) for more information.

**Examples of Possible Analysis Pane Information**

Object	Possible Analysis Information
Node	<ul style="list-style-type: none"> <li>• Summary panel</li> <li>• Interface information and analysis</li> <li>• IP address information and analysis</li> <li>• SNMP information</li> </ul>
Interface	<ul style="list-style-type: none"> <li>• Summary panel</li> <li>• IP address information and analysis</li> </ul>
Incidents	<ul style="list-style-type: none"> <li>• Summary panel</li> <li>• Source Node information and analysis</li> <li>• Source Object information and analysis</li> </ul>

To access the Analysis Pane, select a [workspace](#), click the view that you want to display, and select the row that contains the object.

**Tip:** Some views are also accessible from the console's **Actions** menu. See [Using Actions to Perform Tasks](#) for more information.

**Related Topics**

[Use Table Views](#)

[Use Map Views](#)

## 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 the discovery information for a node:**

1. Do one of the following:

**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 that has the configuration you want to check; for example **Nodes**.

- c. Select the row representing the node that has the configuration you want to check.

**Navigate to a map view and select a node:**

- a. From the workspace navigation panel, select the workspace of interest; for example, **Topology Maps**.
- b. Click the view that contains the node that has the configuration you want to check; for example **Initial Discovery Progress** or **Network Overview**.
- c. From the map view, click the node that has the configuration you want to check.

**Navigate to a Node form:**

- From a table view, double-click the row representing the node that has the configuration you want to see.
- From a map view, click the map icon for the node of interest and click the  Open icon.

2. Select **Actions** → **Polling** → **Configuration Poll**.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

Each time you select **Actions** → **Polling** → **Configuration Poll**, NNMi also applies any Custom Poller Policy that is associated with the selected node. This determines which instances should be polled. See [Configure Custom Polling](#) for more information.

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 Settings Report

Use the **Actions** → **Configuration Details** → **Monitoring Settings** menu item to display the monitoring settings report for a particular object.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

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.

(*NNMi Advanced*) If the Global Network Management feature is enabled and you are signed into a Global Manager:

- Node managed by the Global Manager = **Actions** → **Configuration Details** → **Monitoring Settings** opens a report, provided by the Global Manager (NNMi management server).
- Node managed by a Regional Manager = **Actions** → **Configuration Details** → **Monitoring Settings** accesses that Regional Manager (NNMi management server) and requests the report.

**Note:** You must sign into that Regional Manager unless your network environment enables



Single Sign-On (SSO) to that Regional Manager through the Global Manager. For more information, see the “Configuring Single Sign-On for Global Network Management” section in the *HP Network Node Manager i Software Deployment Reference*, which is available at: <http://h20230.www2.hp.com/selfsolve/manuals>.

(*NNM iSPI Performance for Metrics*) The HP Network Node Manager 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 <code>ifAdminStatus</code> and <code>ifOperStatus</code>. (<code>ifAdminStatus</code> is set by the device administrator. <code>ifOperStatus</code> 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>
Fault Polling Interval	<p>The time that State Poller waits between issuing queries to gather fault information.</p> <p>The default Fault Polling Interval is 5 minutes, except for the Node Group named Microsoft Windows Systems which is 10 minutes.</p>
Performance Polling	<p>(<i>NNM iSPI Performance for Metrics</i>)</p> <p>If enabled, the HP Network Node Manager iSPI Performance for Metrics Software is installed. The NNM iSPI Performance for Metrics 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 HP Network Node Manager iSPI Performance for Metrics Software waits between issuing queries to gather performance information.</p> <p>The default Performance Polling Interval is 5 minutes, except for the Node Group named Microsoft Windows Systems which is 10 minutes.</p>

**To view the monitoring settings report for a Node (SNMP Agent), Interface, IP address, or Card:**

1. Navigate to the view for that object (for example, **Inventory** workspace, **Nodes** view).

2. Select the row representing the object information.
3. Select **Actions** → **Configuration Details** → **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 Members view (for example, **Inventory** workspace, **Router Redundancy Members** view).
2. Select the row representing the Router Redundancy Member of interest.
3. Select **Actions** → **Configuration Details** → **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. Double-click the row representing the Router Redundancy Group of interest.
3. From the Router Redundancy Members tab, double-click the row representing the Router Redundancy Group Member of interest.
4. Select the Tracked Object of interest by selecting the row representing the object information.
5. Select **Actions** → **Configuration Details** → **Monitoring Settings**.

**To view the monitoring configuration for a Node Component:**

1. Navigate to a Node view (for example, **Inventory** workspace, **Nodes** view).
2. Double-click the row representing the Node of interest.
3. Select the **Node Component** tab.
4. Select the Node Component of interest by selecting the row representing the object information.
5. Select **Actions** → **Configuration Details** → **Monitoring Settings**.

**Note:** This menu item is also available on any **Node Component** form.

## View MIB Information for a Node (MIB Browser)

When investigating and diagnosing network problems, you might find it useful to query a node for SNMP responses to obtain information about the node that is not stored in the NNMi database. You can use NNMi's MIB Browser to perform the following tasks:

**Note:** You can view MIB variable information for those nodes to which you have access or for which you provide a valid community string.

"Determine a Node's Supported MIBs (MIB Browser)" on the next page

"Display a MIB File's Contents (MIB Browser)" on page 365

"Determine a Node's MIB Variable Values (MIB Browser)" on page 365

"Display a MIB Table (MIB Browser)" on page 374

"Display MIB Variable Details " on page 367

"Check SNMP Support for a Node (MIB Browser)" on page 377

"Find an Entry in the MIB Browser Output" on page 378

"Export MIB Browser Output " on page 380

"Copy Selected MIB Browser Output (MIB Browser)" on page 382

"Print MIB Browser Output (MIB Browser)" on page 383

See "MIB Browser Keyboard Navigation" below for a description of the keyboard navigation you can use in the MIB Browser.

## MIB Browser Keyboard Navigation

The following table describes the keystrokes you can use to navigate the NNMi MIB Browser.

**Tip:** To incrementally look up values in the first column of a table, type one or more characters that you want to match.

### MIB Browser Keyboard Navigation

Keyboard Key	Description
UP ARROW	Scroll up vertically by one table row.
DOWN ARROW	Scroll down vertically by one table row.
HOME	Move to the first row of the table.
END	Move to the last row of the table.
PAGE UP	Move to the first visible table row.
PAGE DOWN	Move to the last visible table row.
SHIFT + RIGHT ARROW	Open a closed node.
SHIFT + LEFT ARROW	Close an open node.
SPACEBAR	Toggle the table column sort order between ascending and descending order.

## Determine a Node's Supported MIBs (MIB Browser)

To view the MIBs (Management Information Base) supported for a selected Node, use the **Tools** → **List Supported MIBs** option from the MIB Browser. This option is useful when troubleshooting an Incident so that you can determine the kinds of information available for the problem object that is in addition to the information provided in the object's form.

**Note:** You can also view the supported MIBs for a selected Node using the **Actions** → **MIB Information** → **List Supported MIBs** from the NNMi console without accessing the MIB Browser.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

**To view the MIBs supported for a Node from the MIB Browser:**

1. Do one of the following:
  - Select a Node from an Inventory view.
  - Select an Incident from an Incident view.
  - Open a Node or Incident form.

**Note:** NNMi uses the incident's Source Node as the selected Node.
2. Select **Actions** → **MIB Information** → **Browse MIB**.

NNMi displays the MIB Browser.
3. In the **Node** attribute, NNMi displays the name of the Node you selected.
4. *Optional.* In the **Community String** attribute, do one of the following:
  - Leave this attribute value blank. NNMi uses the Communication parameters currently configured in the NNMi database for the specified Node (if any).
  - Enter a valid *read community string* for the Node. NNMi uses default SNMP version, timeout, maximum retries, and port parameters provided by the NNMi administrator within the `nms-ui.properties` file.

For more information, see the "Maintaining NNMi" chapter in the *HP Network Node Manager i Software Deployment Reference*, which is available at:

<http://h20230.www2.hp.com/selfsolve/manuals>.

5. Select **Tools** → **List Supported MIBs**.

NNMi displays the textual representation of the OID (Object Identifier) for each MIB that is supported by the Node's SNMP Agent. When displaying the list, NNMi indicates the MIBs that are supported, but not loaded on the NNMi management server.

To access the MIB form for a supported MIB, click the MIB name, for example `ENTITY-MIB`.

**To view the MIBs supported for a Node without accessing the MIB Browser:**

1. Do one of the following:
  - Select a Node from an Inventory view.
  - Select an Incident from an Incident view.
  - Open a Node or Incident form.

**Note:** NNMi uses the incident's Source Node as the selected Node.
2. Select **Actions** → **MIB Information** → **List Supported MIBs**.

NNMi displays the textual representation of the OID (Object Identifier) for each MIB that is supported by the Node's SNMP Agent. When displaying the list, NNMi indicates the MIBs that are supported, but not loaded.

To access the MIB form for a supported MIB, click the MIB name, for example `ENTITY-MIB`.

## Display a MIB File's Contents (MIB Browser)

To view a MIB (Management Information Base) file's contents, use the **Actions** → **Display MIB File** menu option. This option is useful for examining the contents of an entire MIB file to determine all of the MIB variables and associated values contained in a MIB, or to determine the date the MIB file was last updated.

**Note:** You can also display a MIB file using **Tools** → **Display MIB File** from the MIB Browser.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

**To view a MIB file's contents without accessing the MIB Browser:**

1. Select a MIB Variable from the **Inventory** → **MIB Variables** view.

**Note:** You can also access Actions Display MIB File from the MIB Notification, Table Index, or Enumerated Value form.

2. Select **Actions** → **MIB Information** → **Display MIB File**.

NNMi displays the MIB file's contents.

**To view a MIB file's contents from the MIB Browser:**

1. Select a MIB Variable from the **Inventory** → **MIB Variables** view.

2. Select **Actions** → **MIB Information** → **Browse MIB**.

NNMi displays the MIB Browser.

3. Select **Tools** → **Display MIB File**.

NNMi displays the MIB file's contents for the selected MIB.

## Determine a Node's MIB Variable Values (MIB Browser)

**Tip:** See "MIB Browser Keyboard Navigation" on page 363 for a description of the keyboard navigation you can use in the MIB Browser.

To view MIB (Management Information Base) variable values for the MIB objects supported by the SNMP agent on a specified Node use the **Actions** → **MIB Information** → **Browse MIB** menu item. The MIB variable OID (Object Identifier) value you specify determines the starting point in the MIB for which variable information is retrieved.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

Determining a MIB variable value can be useful when troubleshooting a problem device. For example you might want to view the value of `.1.3.6.1.2.1.1.3 sysUpTime` to determine when the last reboot occurred for a device.

**To view current MIB variable values for a Node:**

1. Do one of the following:
  - Select a Node from an Inventory view.
  - Select an Incident from an Incident view.
  - Open a Node or Incident form.

**Note:** NNMi uses the incident's Source Node as the selected Node.
2. Select **Actions** → **MIB Information** → **Browse MIB**.  
NNMi displays the MIB Browser.
3. In the **Node** attribute, NNMi displays the name of the Node you selected.
4. *Optional.* In the **Community String** attribute, do one of the following:
  - Leave this attribute value blank. NNMi uses the Communication parameters currently configured in the NNMi database for the specified Node (if any).
  - Enter a valid *read community string* for the Node. NNMi uses default SNMP version, timeout, maximum retries, and port parameters provided by the NNMi administrator within the `nms-ui.properties` file.

For more information, see the "Maintaining NNMi" chapter in the *HP Network Node Manager i Software Deployment Reference*, which is available at:

<http://h20230.www2.hp.com/selfsolve/manuals>.

5. In the **OID** attribute, NNMi provides `mib-2.system` (the root of the MIB-2 branch). To change the OID:
  - Type additional numbers or text strings for a specific MIB-2 area.
  - Replace the default OID numbers to issue an SNMP getNext request for another area in the Internet MIB tree.


Note the following:




- To obtain a MIB variable OID value use the **Inventory** → **MIB Variables** view. See ["MIB Variables View" on page 39](#) for more information.
  - The OID must begin with a dot (.).
  - NNMi automatically completes the OID name for you. The name you begin to enter must be one of the following:
    - A valid textual or numeric OID.
    - An OID alias provided by NNMi. To obtain a list of valid OID aliases, use the **Tools** → **OID Aliases** option from the SNMP MIB Browser.
6. Press **Enter**. NNMi does the following:


If the Node responds to SNMP, NNMi displays all responses to MIB objects from any designated starting point down through the Internet MIB tree.

If the associated MIB file is loaded on the NNMi management server, NNMi displays the textual representation of the OID (Object Identifier) for the MIB variable as well as its associated value. If the associated MIB file is not loaded on the NNMi management server, NNMi displays the numeric representation of the OID.

When displaying the value for the MIB variables of type OCTET-STRING, NNMi uses the textual conventions defined in the MIB. If you are an NNMi administrator, see [MIB Textual Conventions Form](#) for more information.

**Note:** You can also click the  Walk button to display MIB Browser output.

7. To expand a MIB or MIB variable entry, do one of the following:
  - Click the  Expand icon that precedes the entry you want to expand.
  - Click **Expand Selected** to expand the selected entries.
8. To collapse a MIB or MIB variable entry, do one of the following:
  - Click the  Collapse icon that precedes the entry you want to collapse.
  - Click **Collapse Selected** to collapse the selected entries.
9. To stop gathering the MIB variable information before NNMi reaches the end of the MIB tree, click the  Stop button.

When all available MIB variable values are displayed, NNMi disables the  Stop button.

## Display MIB Variable Details

**Tip:** See "MIB Browser Keyboard Navigation" on page 363 for a description of the keyboard navigation you can use in the MIB Browser.

To view the MIB Variable details for a selected MIB variable, use the **View** → **Quick View** menu option from the MIB Browser. This option is useful for determining all of the attributes and associated values for the selected MIB variable.

### To view MIB variable details for a selected MIB variable:

1. Access the SNMP MIB Browser.

Do one of the following:

- Select **Tools** → **MIB Browser**.
- **Note:** You can view MIB variable information for those nodes to which you have access or for which you provide a valid community string.
- Open a MIB variable form from the **Inventory** → **MIB Variables** view and select **Actions** → **MIB Information** → **Browse MIB**.

**Note:** You can also access the MIB Browser from a Node or Incident view or form. See [Determine a Node's MIB Variable Values](#) for more information.

NNMi displays the MIB Browser.

2. In the **Node** attribute, enter the Node Name or IP address of the Node that has the MIB variable values you want to view.
3. *Optional.* In the **Community String** attribute, do one of the following:
  - Leave this attribute value blank. NNMi uses the Communication parameters currently configured in the NNMi database for the specified Node (if any).
  - Enter a valid *read community string* for the Node. NNMi uses default SNMP version, timeout, maximum retries, and port parameters provided by the NNMi administrator within the `nms-ui.properties` file.

For more information, see the "Maintaining NNMi" chapter in the *HP Network Node Manager i Software Deployment Reference*, which is available at:

<http://h20230.www2.hp.com/selfsolve/manuals>.

4. In the **OID** attribute, enter the textual or numeric representation of the Object Identifier for the MIB variable to be used as a starting point for viewing the MIB variable values supported on the specified Node. [Click here for more information.](#)

If you accessed the MIB Browser from a MIB variable form, NNMi provides the OID attribute value using the selected MIB variable.

If an OID was not previously selected, NNMi provides `mib-2.system` (the root of the MIB-2 branch). To change the OID:


- Type additional numbers or text strings for a specific MIB-2 area.
- Replace the default OID numbers to issue an SNMP getNext request for another area in the Internet MIB tree.

Note the following:

- To obtain a MIB variable OID value use the **Inventory** → **MIB Variables** view. See ["MIB Variables View " on page 39](#) for more information.
  - The OID must begin with a dot (.).
  - NNMi automatically completes the OID name for you. The name you begin to enter must be one of the following:
    - A valid textual or numeric OID.
    - An OID alias provided by NNMi. To obtain a list of valid OID aliases, use the **Tools** → **OID Aliases** option from the SNMP MIB Browser.
5. Press **Enter**. NNMi does the following:

If the Node responds to SNMP, NNMi displays all responses to MIB objects from any designated starting point down through the Internet MIB tree.

If the associated MIB file is loaded on the NNMi management server, NNMi displays the textual representation of the OID (Object Identifier) for the MIB variable as well as its associated value. If the associated MIB file is not loaded on the NNMi management server, NNMi displays the numeric representation of the OID.

**Note:** You can also click the  Walk button to display MIB Browser output.



6. To expand a MIB or MIB variable entry, do one of the following:
  - Click the ► Expand icon that precedes the entry you want to expand.
  - Click **Expand Selected** to expand the selected entries.
7. To collapse a MIB or MIB variable entry, do one of the following:
  - Click the ▼ Collapse icon that precedes the entry you want to collapse.
  - Click **Collapse Selected** to collapse the selected entries.
8. To stop gathering the MIB variable information before NNMI reaches the end of the Internet MIB tree, click the ● Stop button.

When all available MIB variable values are displayed, NNMI disables the ● Stop button.

9. Select the MIB variable of interest.

**Note:** The MIB variable must have multiple instances. For example: `interfaces.ifTable.ifEntry.ifIndex.1`

10. Select **View** → **Quick View**.

NNMI displays the attribute values for the selected MIB variable. This information is also provided in the MIB Variable form. See "[MIB Variable Form](#)" below for more information.

You can also double-click the MIB variable of interest to access the Quick View details.

## MIB Variable Form

The MIB Variable form enables you to view more detailed information about the MIB variables available from a MIB that is loaded on the NNMI management server.

**For information about each tab:**

**To view MIB variable information for a MIB that is loaded on the NNMI management server:**

1. From the workspace navigation panel, select the **Inventory** workspace.
2. Select **MIB Variables**.
3. Double-click the row of interest.
4. View the Basic attributes (see the [MIB Variable Basic Attributes](#) table)

### MIB Variable Basic Attributes

Attribute	Description
Name	<p>The Name value that is stored in the MIB definition for the selected MIB variable. In the following example, <code>ifAdminStatus</code> is the Name of the MIB variable :</p> <pre> <b>ifAdminStatus</b> OBJECT-TYPE SYNTAX INTEGER { up(1), -- ready to pass packets down(2), testing(3) -- in some test mode }                     </pre>

**MIB Variable Basic Attributes, continued**

Attribute	Description
	ACCESS read-write STATUS mandatory DESCRIPTION "The desired state of the interface. The testing(3) state indicates that no operational packets can be passed." ::= { ifEntry 7 }
OID (Numeric)	The numeric representation of the OID (Object Identification) value for the selected MIB variable.
OID (Text)	The textual representation of the OID for the selected MIB variable.
Syntax	The SYTNAX value for the MIB variable. Valid values for MIB variable that can be included in a MIB Expression include the following: <ul style="list-style-type: none"> <li>• Agent Capabilities (SNMP v2 only)</li> <li>• Bits</li> <li>• Counter</li> <li>• Counter64</li> <li>• Display String (SNMP v1 only)</li> <li>• Enumeration</li> <li>• Gauge</li> <li>• Integer</li> <li>• IP Address</li> <li>• MIB Defined (Indicates a custom type defined in the MIB)</li> <li>• Module Compliance (SNMP v2 only)</li> <li>• Module Identity (SNMP v2 only)</li> <li>• Notification Group (SNMP v2 only)</li> <li>• Notification Type (SNMP v2 only)</li> <li>• Object Group (SNMP v2 only)</li> <li>• Object Identifier</li> <li>• Object Identity (SNMP v2 only)</li> <li>• Octet String</li> <li>• Opaque</li> <li>• Other (Usually indicates the SYNTAX is unset)</li> <li>• Physical Address (SNMP v1 only)</li> <li>• Sequence</li> </ul>

### MIB Variable Basic Attributes, continued

Attribute	Description
	<ul style="list-style-type: none"> <li>• Sequence of</li> <li>• Textual Convention (SNMP v2 only)</li> <li>• Time_Ticks</li> <li>• Unsigned32 (Integer)</li> </ul> <p>For more information, click <a href="#">here</a>.</p> <ul style="list-style-type: none"> <li>• When evaluating MIB expressions that include MIB variables of type Counter, Counter64 or Time_Ticks, NNMi evaluates the MIB Variable using the difference in value between the most recent poll and the poll before it. If you want NNMi to calculate a rate over time in seconds, divide the MIB Expression by sysUptime. For example:   <math display="block">(((ifInOctets+ifOutOctets)*8/ifSpeed) * 100) / sysUpTime * 0.01</math> <p><b>Tip:</b> The sysUpTime variable is a value of hundredths of a second. When you want the rate in seconds, use <code>sysUpTime*0.01</code> in the MIB expression as shown in the previous example.</p> </li> <li>• If you use a MIB variable of type Counter, Counter64 or Time_Ticks in the MIB Expression, NNMi automatically collects sysUpTime values if sysUpTime is not already in the MIB Expression. NNMi uses the sysUptime value to detect a system reboot. Any time a system reboot is detected, NNMi cannot determine the difference in values between polls for any Counter MIB variable and therefore does not calculate the MIB Expression for that poll.</li> </ul>
Textual Convention	Defines the format rules to be used when displaying the MIB value.
MIB	<p>The name value that is stored at the beginning of the MIB definitions to identify the MIB. In the following example, RFC1213-MIB is the name of the MIB:</p> <pre>RFC1213-MIB DEFINITIONS ::= BEGIN</pre>
Description	<p>The Description that is stored in the MIB for the selected MIB variable. The following example includes the description for ifAdminStatus in the RFC1213-MIB:</p> <pre>ifAdminStatus OBJECT-TYPE SYNTAX INTEGER {   up(1), -- ready to pass packets   down(2),   testing(3) -- in some test mode }  ACCESS read-write STATUS mandatory DESCRIPTION   "The desired state of the interface. The testing(3) state   indicates</pre>

### MIB Variable Basic Attributes, continued

Attribute	Description
	that no operational packets can be passed." ::= { ifEntry 7 }

### Enumerated Values Form

The Enumerated Values form enables you to view each enumerated value pair, if any, for a selected MIB variable. For example, the `ifAdminStatus` MIB variable, includes enumerated values for status as shown in the following example:

```
ifAdminStatus OBJECT-TYPE
SYNTAX INTEGER {
1 up
2 down
3 testing(3)
}

ACCESS read-write
STATUS mandatory
DESCRIPTION
"The desired state of the interface. The testing(3) state
indicates that no operational packets can be passed."
 ::= { ifEntry 7 }
```

The enumerated values are included in the following table:

#### Enumerated Values for ifAdminStatus

String Value	Numeric Value
up	1
down	2
testing	3

**For information about each tab:**

**To view the enumerated values for a selected MIB variable:**

1. From the workspace navigation panel, select the **Inventory** workspace.
2. Select **MIB Variables**.
3. Double-click the row of interest.
4. Select the **Enumerated Values** tab.

NNMi displays the string and numeric value for each enumeration, if any, specified for the selected MIB variable.

5. To view more details about an enumerated value pair, double-click the row of interest.

6. View the Basics information for the selected Enumerated Value (see the [Enumerated Value Basic Attributes](#) table).

### Enumerated Value Basic Attributes

Attribute	Description
String Value	The text value that is associated with the Numeric Value for the selected MIB variable.
Numeric Value	The numeric value that is associated with the String Value for the selected MIB variable.
MIB Variable	The name of the selected MIB variable that contains enumerated values. For example, <code>ifAdminStatus</code> is a MIB Variable that contains enumerated values.
MIB	The name value that is stored at the beginning of the MIB definitions to identify the MIB. In the following example, <code>RFC1213-MIB</code> is the name of the MIB:  <code>RFC1213-MIB DEFINITIONS ::= BEGIN</code>

### Table Indices Form

The Table Index form enables you to view the index values, if any, for a selected MIB variable. Table indices are identified using the INDEX keyword as shown in the following example for the `atEntry` MIB variable:

```
atEntry OBJECT-TYPE
  SYNTAX AtEntry
  ACCESS not-accessible
  STATUS deprecated
  DESCRIPTION
    "Each entry contains one NetworkAddress to
    `physical' address equivalence."
  INDEX { atIfIndex,
  atNetAddress }
  ::= { atTable 1 }
```

In the example, `atIfIndex` and `atNetAddress` are table indices for the `atEntry` MIB variable.

Table indices are used to store multiple values for a single MIB variable.

#### For information about each tab:

#### To view the table index values for a selected MIB variable:

1. From the workspace navigation panel, select the **Inventory** workspace.
2. Select **MIB Variables**.
3. Double-click the row of interest.
4. Navigate to the **Table Indices** tab.

NNMi displays the Position and Name for each of the Table Indices, if any, specified for the selected MIB variable.

5. To view more details about a specific Table Index entry, double-click the row of interest.
6. View the Basics information for the selected Table Index (see the [Table Index Basic Attributes](#) table).

### Table Index Basic Attributes

Attribute	Description
Position	The position number of the MIB variable that is used as a Table Index object. In the following example, <code>atIfIndex</code> and <code>atNetAddress</code> are MIB Variables used as Table Index objects. <code>atIfIndex</code> is position 0 and <code>atNetAddress</code> is position 1:  <pre>INDEX { <b>atIfIndex</b>, <b>atNetAddress</b> }</pre>
MIB Variable	The name of the selected MIB variable that is used as a Table Index object. Table indices are used for storing multiple values for a MIB variable.
Table Definition	The name of the MIB variable used to define the MIB table. In the following example, <code>atEntry</code> is the MIB variable that defines the MIB table:  <pre><b>atEntry</b> OBJECT-TYPE SYNTAX AtEntry ACCESS not-accessible STATUS deprecated DESCRIPTION "Each entry contains one NetworkAddress to `physical' address equivalence." INDEX { atIfIndex, atNetAddress } ::= { atTable 1 }</pre>
MIB Name	The name value that is stored at the beginning of the MIB definitions to identify the MIB. In the following example, <code>RFC1213-MIB</code> is the name of the MIB:  <pre>RFC1213-MIB DEFINITIONS ::= BEGIN</pre>

## Display a MIB Table (MIB Browser)

**Tip:** See "MIB Browser Keyboard Navigation" on page 363 for a description of the keyboard navigation you can use in the MIB Browser.

To view the MIB table for a selected MIB variable, use the **View** → **MIB Table** menu option from the MIB Browser. This option is useful for determining all of the attributes and associated values for each instance of the MIB variable in a MIB table.

### To view MIB table information for a selected MIB variable:

1. Access the MIB Browser.  
 Do one of the following:
  - Select **Tools** → **MIB Browser**.
  - **Note:** You can view MIB variable information for those nodes to which you have access or

for which you provide a valid community string.

- Open a MIB variable form from the **Inventory** → **MIB Variables** view and select **Actions** → **MIB Information** → **Browse MIB**.

**Note:** You can also access the MIB Browser from a node or incident view or form. See [Determine a Node's MIB Variable Values](#) for more information.

NNMi displays the MIB Browser.

2. In the **Node** attribute, enter the node name or IP address of the node that has the MIB variable values you want to view.
3. *Optional.* In the **Community String** attribute, do one of the following:
  - Leave this attribute value blank. NNMi uses the Communication parameters currently configured in the NNMi database for the specified Node (if any).
  - Enter a valid *read community string* for the Node. NNMi uses default SNMP version, timeout, maximum retries, and port parameters provided by the NNMi administrator within the `nms-ui.properties` file.

For more information, see the "Maintaining NNMi" chapter in the *HP Network Node Manager i Software Deployment Reference*, which is available at:

<http://h20230.www2.hp.com/selfsolve/manuals>.

4. In the **OID** attribute, enter the textual or numeric representation of the Object Identifier for the MIB variable to be used as a starting point for viewing the MIB variable values supported on the specified node. Click [here](#) for more information.

If you accessed the MIB Browser from a MIB variable form, NNMi provides the OID attribute value using the selected MIB variable.

If an OID was not previously selected, NNMi provides `mib-2.system` (the root of the MIB-2 branch). To change the OID:

- Type additional numbers or text strings for a specific MIB-2 area.
- Replace the default OID numbers to issue an SNMP getNext request for another area in the Internet MIB tree.




Note the following:

- To obtain a MIB variable OID value use the **Inventory** → **MIB Variables** view. See ["MIB Variables View " on page 39](#) for more information.
  - The OID must begin with a dot (.).
  - NNMi automatically completes the OID name for you. The name you begin to enter must be one of the following:
    - A valid textual or numeric OID.
    - An OID alias provided by NNMi. To obtain a list of valid OID aliases, use the **Tools** → **OID Aliases** option from the SNMP MIB Browser.
5. Press **Enter**. NNMi does the following:

If the Node responds to SNMP, NNMi displays all responses to MIB objects from any designated starting point down through the Internet MIB tree.

If the associated MIB file is loaded on the NNMi management server, NNMi displays the textual representation of the OID (Object Identifier) for the MIB variable as well as its associated value. If the associated MIB file is not loaded on the NNMi management server, NNMi displays the numeric representation of the OID.


**Note:** You can also click the  Start SNMP Walk button to display MIB Browser output.

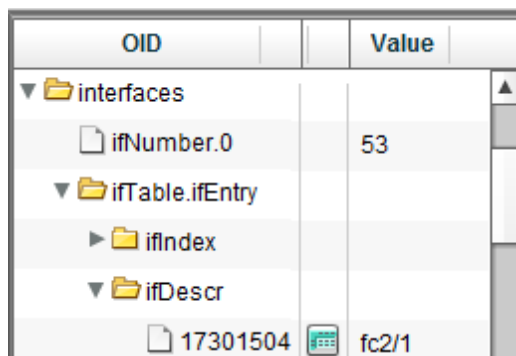
6. To expand a MIB or MIB variable entry, do one of the following:
  - Click the  Expand icon that precedes the entry you want to expand.
  - Click **Expand Selected** to expand the selected entries.
7. To collapse a MIB or MIB variable entry, do one of the following:
  - Click the  Collapse icon that precedes the entry you want to collapse.
  - Click **Collapse Selected** to collapse the selected entries.
8. To stop gathering the MIB variable information before NNMi reaches the end of the Internet MIB tree, click the  Stop SNMP Walk button.


When all available MIB variable values are displayed, NNMi disables the  Stop SNMP Walk button.



9. Select the MIB variable of interest.

Note the following:

- The MIB Variable must have multiple instances. For example: `interfaces.ifTable.ifEntry.ifIndex.1`
- NNMi uses the  View MIB Table button to indicate MIB Variables that have multiple instances.



OID	Value
▼ interfaces	
ifNumber.0	53
▼ ifTable.ifEntry	
▶ ifIndex	
▼ ifDescr	
17301504 	fc2/1

10. To view the MIB table of multiple instances, click the  View MIB Table button or select a row that contains a  View MIB Table button and click **View** → **MIB Table**.

NNMi displays the MIB table that is associated with the selected MIB Variable. The MIB table includes all of the attributes and associated values for each instance in the MIB table.



## Check SNMP Support for a Node (MIB Browser)

**Tip:** See "MIB Browser Keyboard Navigation" on page 363 for a description of the keyboard navigation you can use in the MIB Browser.

In addition to determining the MIBs and MIB variables supported for a node, you can use the MIB Browser to check the following:

- Whether a node supports SNMP
- Valid SNMP community strings

### To check SNMP support for a selected node:

1. Do one of the following:
  - Select a Node from an Inventory view.
  - Select an Incident from an Incident view.
  - Open a Node or Incident form.

**Note:** NNMi uses the incident's Source Node as the selected Node.

2. Select **Actions** → **MIB Information** → **Browse MIB**.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

NNMi displays the MIB Browser.

3. In the **OID** attribute, NNMi provides `mib-2.system` (the root of the MIB-2 branch). To change the OID:
  - Type additional numbers or text strings for a specific MIB-2 area.
  - Replace the default OID numbers to issue an SNMP getNext request for another area in the Internet MIB tree.

Click here for more information. Note the following:

- To obtain a MIB variable OID value use the **Inventory** → **MIB Variables** view. See "MIB Variables View" on page 39 for more information.
  - The OID must begin with a dot (.).
  - NNMi automatically completes the OID name for you. The name you begin to enter must be one of the following:
    - A valid textual or numeric OID.
    - An OID alias provided by NNMi. To obtain a list of valid OID aliases, use the **Tools** → **OID Aliases** option from the SNMP MIB Browser.
4. *Optional.* In the **Community String** attribute, do one of the following:
    - Leave this attribute value blank. NNMi uses the Communication parameters currently configured in the NNMi database for the specified Node (if any).


- Enter a valid *read community string* for the Node. NNMi uses default SNMP version, timeout, maximum retries, and port parameters provided by the NNMi administrator within the `nms-ui.properties` file.

For more information, see the "Maintaining NNMi" chapter in the *HP Network Node Manager i Software Deployment Reference*, which is available at:

<http://h20230.www2.hp.com/selfsolve/manuals>.

5. Press **Enter**. NNMi does the following:

- If the Node responds to SNMP, NNMi displays all responses to MIB objects from any designated starting point down through the Internet MIB tree.
- If the associated MIB file is loaded on the NNMi management server, NNMi displays the textual representation of the OID (Object Identifier) for the MIB variable as well as its associated value. If the associated MIB file is not loaded on the NNMi management server, NNMi displays the numeric representation of the OID.

**Note:** You can also click the  Walk button to display MIB Browser output.

## Find an Entry in the MIB Browser Output

**Tip:** See "MIB Browser Keyboard Navigation" on page 363 for a description of the keyboard navigation you can use in the MIB Browser.

When using the MIB Browser to determine MIBs and MIB variables supported for a node, use the MIB Browser **Find** button to search for a particular text string within the output. For example, you might want to search for a specific MIB variable without examining all of the MIB Browser output.

**To find a text string in the MIB Browser output:**

1. Access the MIB Browser.

Do one of the following:

Select **Tools** → **MIB Browser**.

- **Note:** You can view MIB variable information for those nodes to which you have access or for which you provide a valid community string.
- Open a MIB variable form from the **Inventory** → **MIB Variables** view and select **Actions** → **MIB Information** → **Browse MIB**.

**Note:** You can also access the MIB Browser from a node or incident view or form. See [Determine a Node's MIB Variable Values](#) for more information.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

NNMi displays the MIB Browser.

2. In the **OID** attribute, enter the textual or numeric representation of the Object Identifier for the MIB variable to be used as a starting point for viewing the MIB variable values supported on the specified node. Click here for more information.

If you accessed the MIB Browser from a MIB variable form, NNMi provides the OID attribute value using the selected MIB variable.

If an OID was not previously selected, NNMi provides `mib-2.system` (the root of the MIB-2 branch). To change the OID:

- Type additional numbers or text strings for a specific MIB-2 area.
- Replace the default OID numbers to issue an SNMP getNext request for another area in the Internet MIB tree.

Note the following:

- To obtain a MIB variable OID value use the **Inventory** → **MIB Variables** view. See "[MIB Variables View](#)" on page 39 for more information.
- The OID must begin with a dot (.).
- NNMi automatically completes the OID name for you. The name you begin to enter must be one of the following:
  - A valid textual or numeric OID.
  - An OID alias provided by NNMi. To obtain a list of valid OID aliases, use the **Tools** → **OID Aliases** option from the SNMP MIB Browser.

3. *Optional.* In the **Community String** attribute, do one of the following:

- Leave this attribute value blank. NNMi uses the Communication parameters currently configured in the NNMi database for the specified Node (if any).
- Enter a valid *read community string* for the Node. NNMi uses default SNMP version, timeout, maximum retries, and port parameters provided by the NNMi administrator within the `nms-ui.properties` file.

For more information, see the "Maintaining NNMi" chapter in the *HP Network Node Manager i Software Deployment Reference*, which is available at:

<http://h20230.www2.hp.com/selfsolve/manuals>.


4. Press **Enter**. NNMi does the following:

If the node responds to SNMP, NNMi displays all responses to MIB objects from any designated starting point down through the Internet MIB tree.


If the associated MIB file is loaded on the NNMi management server, NNMi displays the textual representation of the OID (Object Identifier) for the MIB variable as well as its associated value. If the associated MIB file is not loaded on the NNMi management server, NNMi displays the numeric representation of the OID.

**Note:** You can also click the  Walk button to display MIB Browser output.


5. Expand the MIB or MIB variable entries in which you want search:


- Click the  Expand icon that precedes the entry you want to expand.
- Click **Expand Selected** to expand the selected entries listed.

6. To collapse a MIB or MIB variable entry, do one of the following:

- Click the  Collapse icon that precedes the entry you want to collapse.
- Click **Collapse Selected** to collapse the selected entries listed.

7. To stop gathering the MIB variable information before NNMi reaches the end of the Internet

MIB tree, click the  Stop button.

When all available MIB variable values are displayed, NNMi disables the  Stop button.

8. To find a text string, enter the text string value in the field next to the Find button and click **Find**.

NNMi searches all of the expanded OID column entries and highlights the first occurrence of the text string you enter.

Each time you click **Find**, NNMi advances to the next occurrence of the text string you entered.

## Export MIB Browser Output

In addition to determining the MIBs and MIB variables supported for a node, you can use the MIB Browser to export the SNMP query results to another application. For example, you might want to place the contents in a spreadsheet.

NNMi exports your SNMP query results in a comma-delimited format to the Clipboard. You can then paste the output to any application that accepts the comma-delimited format.

If you do not need a comma-delimited format, use **Edit** → **Copy** when you want to select output for printing or pasting to another application. See "[Copy Selected MIB Browser Output \(MIB Browser\)](#)" on page 382 for more information.

Use **File** → **Print Visible** when you want to generate a printout of the output without using it in another application. See "[Print MIB Browser Output \(MIB Browser\)](#)" on page 383 for more information.

### To export the MIB Browser output :

1. Access the MIB Browser.

Do one of the following:

Select **Tools** → **MIB Browser**.

- **Note:** You can view MIB variable information for those nodes to which you have access or for which you provide a valid community string.
- Open a MIB variable form from the **Inventory** → **MIB Variables** view and select **Actions** → **MIB Information** → **Browse MIB**.

**Note:** You can also access the MIB Browser from a node or incident view or form. See [Determine a Node's MIB Variable Values](#) for more information.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

NNMi displays the MIB Browser.

2. In the **Node** attribute, NNMi displays the name of the node you selected.
3. *Optional.* In the **Community String** attribute, do one of the following:

- Leave this attribute value blank. NNMi uses the Communication parameters currently configured in the NNMi database for the specified Node (if any).
- Enter a valid *read community string* for the Node. NNMi uses default SNMP version, timeout, maximum retries, and port parameters provided by the NNMi administrator within the `nms-ui.properties` file.

For more information, see the "Maintaining NNMi" chapter in the *HP Network Node Manager i Software Deployment Reference*, which is available at:

<http://h20230.www2.hp.com/selfsolve/manuals>.

4. In the **OID** attribute, enter the textual or numeric representation of the Object Identifier for the MIB variable to be used as a starting point for viewing the MIB variable values supported on the specified node. Click here for more information.

If you accessed the MIB Browser from a MIB variable form, NNMi provides the OID attribute value using the selected MIB variable.

If an OID was not previously selected, NNMi provides `mib-2.system` (the root of the MIB-2 branch). To change the OID:

- Type additional numbers or text strings for a specific MIB-2 area.
- Replace the default OID numbers to issue an SNMP getNext request for another area in the Internet MIB tree.

Note the following:

- To obtain a MIB variable OID value use the **Inventory** → **MIB Variables** view. See "[MIB Variables View](#)" on page 39 for more information.
  - The OID must begin with a dot (.).
  - NNMi automatically completes the OID name for you. The name you begin to enter must be one of the following:
    - A valid textual or numeric OID.
    - An OID alias provided by NNMi. To obtain a list of valid OID aliases, use the **Tools** → **OID Aliases** option from the SNMP MIB Browser.
5. Press **Enter**. NNMi does the following:

If the node responds to SNMP, NNMi displays all responses to MIB objects from any designated starting point down through the Internet MIB tree.

If the associated MIB file is loaded on the NNMi management server, NNMi displays the textual representation of the OID (Object Identifier) for the MIB variable as well as its associated value. If the associated MIB file is not loaded on the NNMi management server, NNMi displays the numeric representation of the OID.

**Note:** You can also click the  Walk button to display MIB Browser output.

6. Select **File** → **Export to Clipboard**.

NNMi exports your SNMP query results in a comma-delimited format to the Clipboard. You can then paste the output to any application that accepts the comma-delimited format.

**Note:** All data that is available from the query is exported.

## Copy Selected MIB Browser Output (MIB Browser)

**Tip:** See "MIB Browser Keyboard Navigation" on page 363 for a description of the keyboard navigation you can use in the MIB Browser.

In addition to determining the MIBs and MIB variables supported for a node, you can use the MIB Browser to copy the output to another application. For example, you might want to send the contents to a coworker or save it for later comparison.

When you need a comma-delimited format, use the **File** → **Export to Clipboard** option.

**To copy the MIB Browser output for a selected node:**

1. Access the MIB Browser.

Do one of the following:

Select **Tools** → **MIB Browser**.

- **Note:** You can view MIB variable information for those nodes to which you have access or for which you provide a valid community string.
- Open a MIB variable form from the **Inventory** → **MIB Variables** view and select **Actions** → **MIB Information** → **Browse MIB**.

**Note:** You can also access the MIB Browser from a node or incident view or form. See [Determine a Node's MIB Variable Values](#) for more information.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

NNMi displays the MIB Browser.

2. In the **Node** attribute, NNMi displays the name of the node you selected.
3. *Optional.* In the **Community String** attribute, do one of the following:
  - Leave this attribute value blank. NNMi uses the Communication parameters currently configured in the NNMi database for the specified Node (if any).
  - Enter a valid *read community string* for the Node. NNMi uses default SNMP version, timeout, maximum retries, and port parameters provided by the NNMi administrator within the `nms-ui.properties` file.

For more information, see the "Maintaining NNMi" chapter in the *HP Network Node Manager i Software Deployment Reference*, which is available at:

<http://h20230.www2.hp.com/selfsolve/manuals>.

4. In the **OID** attribute, enter the textual or numeric representation of the Object Identifier for the MIB variable to be used as a starting point for viewing the MIB variable values supported on the specified node. Click here for more information.

If you accessed the MIB Browser from a MIB variable form, NNMi provides the OID attribute value using the selected MIB variable.

If an OID was not previously selected, NNMi provides `mib-2.system` (the root of the MIB-2 branch). To change the OID:

- Type additional numbers or text strings for a specific MIB-2 area.
- Replace the default OID numbers to issue an SNMP getNext request for another area in the Internet MIB tree.


Note the following:




- To obtain a MIB variable OID value use the **Inventory** → **MIB Variables** view. See ["MIB Variables View" on page 39](#) for more information.
- The OID must begin with a dot (.).
- NNMi automatically completes the OID name for you. The name you begin to enter must be one of the following:
  - A valid textual or numeric OID.
  - An OID alias provided by NNMi. To obtain a list of valid OID aliases, use the **Tools** → **OID Aliases** option from the SNMP MIB Browser.


5. Press **Enter**. NNMi does the following:

If the Node responds to SNMP, NNMi displays all responses to MIB objects from any designated starting point down through the Internet MIB tree.

If the associated MIB file is loaded on the NNMi management server, NNMi displays the textual representation of the OID (Object Identifier) for the MIB variable as well as its associated value. If the associated MIB file is not loaded on the NNMi management server, NNMi displays the numeric representation of the OID.

**Note:** You can also click the  Walk button to display MIB Browser output.

6. To expand a MIB or MIB variable entry, do one of the following:
  - Click the  Expand icon that precedes the entry you want to expand.
  - Click **Expand Selected** to expand the selected entries.
7. To collapse a MIB or MIB variable entry, do one of the following:
  - Click the  Collapse icon that precedes the entry you want to collapse.
  - Click **Collapse Selected** to collapse the selected entries.
8. To stop gathering the MIB variable information before NNMi reaches the end of the Internet MIB tree, click the  Stop button.

When all available MIB variable values are displayed, NNMi disables the  Stop button.

9. Select the text you want to copy.
10. Select **Edit** → **Copy**.

NNMi copies the selected output to the Clipboard. You can then paste the output to any application that accepts the text output.

## Print MIB Browser Output (MIB Browser)

**Tip:** See ["MIB Browser Keyboard Navigation" on page 363](#) for a description of the keyboard navigation you can use in the MIB Browser.

You can print MIB Browser output using the MIB Browser's **File** menu. NNMi enables you to print either the entire output contents or only the visible content.

**To print MIB Browser output for a selected node:**

1. Access the MIB Browser.

Do one of the following:

Select **Tools** → **MIB Browser**.

- **Note:** You can view MIB variable information for those nodes to which you have access or for which you provide a valid community string.
- Open a MIB variable form from the **Inventory** → **MIB Variables** view and select **Actions** → **MIB Information** → **Browse MIB**.

**Note:** You can also access the MIB Browser from a node or incident view or form. See [Determine a Node's MIB Variable Values](#) for more information.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

NNMi displays the MIB Browser.

2. In the **Node** attribute, NNMi displays the name of the node you selected.
3. *Optional.* In the **Community String** attribute, do one of the following:
  - Leave this attribute value blank. NNMi uses the Communication parameters currently configured in the NNMi database for the specified Node (if any).
  - Enter a valid *read community string* for the Node. NNMi uses default SNMP version, timeout, maximum retries, and port parameters provided by the NNMi administrator within the `nms-ui.properties` file.

For more information, see the "Maintaining NNMi" chapter in the *HP Network Node Manager i Software Deployment Reference*, which is available at:

<http://h20230.www2.hp.com/selfsolve/manuals>.

4. In the **OID** attribute, enter the textual or numeric representation of the Object Identifier for the MIB variable to be used as a starting point for viewing the MIB variable values supported on the specified node. Click here for more information.

If you accessed the MIB Browser from a MIB variable form, NNMi provides the OID attribute value using the selected MIB variable.

If an OID was not previously selected, NNMi provides `mib-2.system` (the root of the MIB-2 branch). To change the OID:

- Type additional numbers or text strings for a specific MIB-2 area.
- Replace the default OID numbers to issue an SNMP getNext request for another area in the Internet MIB tree.

Note the following:





- To obtain a MIB variable OID value use the **Inventory** → **MIB Variables** view. See ["MIB Variables View" on page 39](#) for more information.
- The OID must begin with a dot (.).




- NNMi automatically completes the OID name for you. The name you begin to enter must be one of the following:
  - A valid textual or numeric OID.
  - An OID alias provided by NNMi. To obtain a list of valid OID aliases, use the **Tools** → **OID Aliases** option from the SNMP MIB Browser.
- 5. Press **Enter**. NNMi does the following:

If the node responds to SNMP, NNMi displays all responses to MIB objects from any designated starting point down through the Internet MIB tree.

If the associated MIB file is loaded on the NNMi management server, NNMi displays the textual representation of the OID (Object Identifier) for the MIB variable as well as its associated value. If the associated MIB file is not loaded on the NNMi management server, NNMi displays the numeric representation of the OID.

**Note:** You can also click the  Walk button to display MIB Browser output.
- 6. To expand a MIB or MIB variable entry, do one of the following:
  - Click the  Expand icon that precedes the entry you want to expand.
  - Click **Expand Selected** to expand the selected entries.
- 7. To collapse a MIB or MIB variable entry, do one of the following:
  - Click the  Collapse icon that precedes the entry you want to collapse.
  - Click **Collapse Selected** to collapse the selected entries.
- 8. To stop gathering the MIB variable information before NNMi reaches the end of the Internet MIB tree, click the  Stop button.

When all available MIB variable values are displayed, NNMi disables the  Stop button.
- 9. To print only the visible content, select **File** → **Print Visible**.

NNMi prints the output to the printer you specify.

## Verify Current Status of a Device

NNMi calculates the status of devices each time additional information is gathered. 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).

**Note:** Using **Actions** → **Polling** → **Status Poll** does not affect the timing of the Polling interval configured for the device.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

### To update node status information:

1. Navigate to the view of interest and select each node that has the 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 that has the status you want to update; for example **Nodes**.
- c. From the table view, press CTRL-Click and select each row that represents a node that has a 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. CTRL-click each node that has a 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, press CTRL-Click and select each row that represents an incident that has the Source Node status you want to update (maximum 10).

2. Select **Actions** → **Polling** → **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 displays: <ul style="list-style-type: none"> <li>■ If the target is responding.</li> <li>■ If the poll was successful.</li> <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 47](#). Check the information displayed on the ["Node Form: Status Tab" on page 75](#) and the ["Node Form: Node Components Tab" on page 69](#).
- Check the Node icon status colors on maps (["Watch Status Colors" on page 285](#)).

- In a Node view, locate the row representing the node and check the icon in the Status column.
- From the Incident form, open the Source Node's form, see "[Incident Form](#)" on page 311 for instructions about using the Source Node attribute to open the appropriate Node form.

## Interpret Root Cause Incidents

**Tip:** Also see "[Investigate and Diagnose Problems](#)" on page 355 for more information about troubleshooting tools that NNMi provides.


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
-  Warning
-  Minor
-  Major
-  Critical
-  Disabled
-  Unknown

**Incident form** explains 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 404 )
- A node or connection might be down and need your attention (see "[Node or Connection Down](#)" on page 406)
- An interface is operationally down (see "[Interface Down](#)" on page 401)
- An address is no longer responding (see "[Address Not Responding](#)" on the next page).
- The connection between two important devices is down (see "[Connection Down](#)" on page 397)

For more information about a specific root cause incident:

To access an incident form from the **Incident Management** or **Incident Browsing** workspace, click the  Open icon in the row representing an incident. The "[Incident Form](#)" on page 311 displays all details about the selected incident.

The **SNMP Trap Configuration**, **Remote NNM 6.x/7.x Event Configuration**, or **Management Event Configuration** form provides a way to view an incident configuration's Description. The Incident Description attribute includes information about the reasons the incident occurred. The

Incident configuration form also includes any additional configurations specified for the incident. For example, the NNMI administrator might have specified an Enrichment configuration to customize incident attributes, such as an incident's Message Format or Severity. After selecting or opening an incident, use **Actions** → **Open Incident configuration** to display an incident's configuration.

**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 285 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.

## Address Not Responding

NNMI periodically uses an ICMP ping command to check each address. If there is no response and the node is not completely unreachable, NNMI's Causal Engine determines that the address is not responding.

On the Source Object form, NNMI updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>AddressNotResponding</b> Conclusion.
Incident	Adds the <b>Address Not Responding</b> incident.
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

On the Source Node form, NNMI updates information on the following tabs:

### Source Node Updates

Tab	Description
Addresses	Changes the State and Status of the address to <b>Critical</b> .
Status	Adds the <b>Minor</b> Status.
Conclusion	<b>SomeUnresponsiveAddressesInNode</b> <b>Note:</b> If you view an <b>AllUnresponsiveAddressesInNode</b> Conclusion, see " <a href="#">Node Down</a> " on page 404 for more information.

On the maps, the icon for the Source Node is set to yellow.

When the IP Address starts responding to ICMP and NNMI can reach the node, NNMI updates the following attributes:

- The IP Address Status is changed to **Normal**.
- The IP Address Conclusion is changed to AddressResponding.

- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.
- The Node Status is changed to **Normal**. The Conclusion on the Node is ResponsiveAddressInNode.

## Aggregator Interface Degraded (NNMi Advanced)

**Link Aggregation**<sup>1</sup>: NNMi generates an **Aggregator Interface Degraded** incident when the Status of at least one of the Aggregation Member Interfaces 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 Source Object form, NNMi updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>AggregatorDegraded</b> Conclusion.
Incident	Adds the <b>Aggregator Interface Degraded</b> incident.  The <b>Correlated Children</b> tab has an <b>Interface Down</b> incident for the member interfaces that have a Status of <b>Critical</b> .
Status	Adds the <b>Minor</b> Status.
Overall Status	Changes to <b>Minor</b> .

On the Source Node form, NNMi updates information on the following tabs:

### Source Node Updates

Tab	Description
Interfaces	Changes the State and Status of all member interfaces that have an Operational State of Down to <b>Critical</b> .
Status	Adds the <b>Minor</b> Status.
Conclusions	<b>InterfacesDownInNode</b>

See "Interface Down" on page 401 for more information about Interface Down incidents.

On Layer 2 Neighbor View maps, the icon for the Aggregator Interface is yellow:

---

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.



When an Interface Up occurs for all of the Aggregation Member Interfaces that have a Status of **Critical**, NNMi updates the following attributes:

- Each Aggregator Interface Status is changed to **Normal**.
- Each Aggregator Interface Conclusion is changed to AggregatorUp.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.

## Aggregator Interface Down (NNMi Advanced)

**Link Aggregation**<sup>1</sup>: NNMi generates an **Aggregator Interface Down** when the Status of all Aggregation Member Interfaces are set to **Critical**.

An Aggregator Interface might 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 participating Aggregation Member Interfaces 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 Source Object form, NNMi updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>AggregatorDown</b> Conclusion.
Incident	Adds the <b>Aggregator Interface Down</b> incident. The <b>Correlated Children</b> tab has an <b>Interface Down</b> incident for the member interfaces that have a Status of <b>Critical</b> .
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

On the Source Node form, NNMi updates information on the following tabs:

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

### Source Node Updates

Tab	Description
Interfaces	Changes the State and Status of all member interfaces that have an Operational State of Down to <b>Critical</b> .
Status	Adds the <b>Minor</b> Status.
Conclusions	<b>InterfacesDownInNode</b>

See "Interface Down" on page 401 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 the Aggregation Interfaces that have a Status of **Critical**, NNMi updates the following attributes:

- The Aggregator Interface Status is changed to **Normal**.
- The Aggregator Interface Conclusion is changed to AggregatorUp.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.

## Aggregator Connection Degraded (NNMi Advanced)

**Link Aggregation**<sup>1</sup>: NNMi generates an **Aggregator Connection Degraded** incident when the Status of at least one of the Aggregator Interfaces (at either end of the connection) is set to **Minor**. See [Layer 2 Neighbor View Map Objects](#) for more information about Aggregator Interfaces and Aggregator Layer 2 Connections. Also see "Aggregator Interface Degraded (NNMi Advanced)" on page 389.

An Aggregator Connection Degraded incident has a Severity set to **Minor**.

On the Source Object form, NNMi updates information on the following tabs:

---

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>AggregatorLinkDegraded</b> Conclusion.
Incident	Adds the <b>Aggregator Connection Degraded</b> incident. The <b>Correlated Children</b> tab has an <b>Aggregator Degraded</b> incident for each Aggregator Interface.
Status	Adds the <b>Minor</b> Status.
Overall Status	Changes to <b>Minor</b> .

On the Source Node form, NNMi updates information on the following tabs:

### Source Node Updates

Tab	Description
Interfaces	Changes the State and Status of all Aggregation Member Interfaces that have an Operational State of Down to <b>Critical</b> .
Status	Adds the <b>Minor</b> Status.
Conclusions	<b>InterfacesDownInNode</b>

See "Interface Down" on page 401 for more information about Interface Down incidents.

On Layer 2 Neighbor View maps, the icon for the Aggregator Layer 2 Connection is yellow:



When NNMi determines that all Aggregator Interfaces in an Aggregator Connection are up, NNMi updates the following attributes:

- The Aggregator Connection Status is changed to **Normal**.
- The Aggregator Connection Conclusion is changed to AggregatorLinkUp.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.



## Aggregator Connection Down (NMMi Advanced)

**Link Aggregation**<sup>1</sup>: NMMi generates an **Aggregator Connection Down** incident when the Status of at least one of the Aggregator Interfaces is set to **Critical**. See [Layer 2 Neighbor View Map Objects](#) for more information about Aggregator Interfaces and Aggregator Layer 2 Connections. Also see "[Aggregator Interface Down \(NMMi Advanced\)](#)" on page 390.

An Aggregator Connection Down incident has Severity set to **Critical**.

On the Source Object form NMMi updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>AggregatorLinkDown</b> Conclusion.
Incident	Adds the <b>Aggregator Connection Down</b> incident.  The <b>Correlated Children</b> tab includes the <b>Aggregator Down</b> incidents under this incident.
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

On the Source Node form, NMMi updates information on the following tabs:

### Source Node Updates

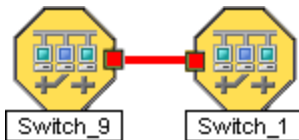
Tab	Description
Interfaces	Changes the State and Status of all member interfaces that have an Operational State of Down to <b>Critical</b> .
Status	Adds the <b>Minor</b> Status.
Conclusions	<b>InterfacesDownInNode</b>

See "[Interface Down](#)" on page 401 for more information about Interface Down incidents.

On Layer 2 Neighbor View maps, the icon for the Aggregator Connection is red:

---

<sup>1</sup>Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.



When NNMi determines that all Aggregator Interfaces in an Aggregator Connection are up, NNMi updates the following attributes:

- The Aggregator Connection Status is changed to **Normal**.
- The Aggregator Connection Conclusion is changed to AggregatorLinkUp.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 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 Object form, NNMi updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>BufferOutOfRangeOrMalfunctioning</b> Conclusion.
Incident	Adds the <b>Buffer has Insufficient Capacity or is Malfunctioning</b> incident. The <b>Correlated Children</b> tab includes any associated traps.
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

The Source Node map icon does not change color because this incident does not affect Node Status.

When NNMi determines that the buffer is functioning properly, NNMi updates the following attributes:

- The Node Status is changed to **Normal**.
- The Node Conclusion is changed to BufferInRangeAndFunctioning.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.

## Card Disabled

**Note:** **Card Disabled** incidents are disabled by default. If you are an NNMi administrator, see [Generate Card Disabled Incidents](#) for information about how to enable this incident.

NNMi periodically uses SNMP to check each card. If an SNMP agent reports that a card has an Administrative State of Down, NNMi's Causal Engine takes the following actions.

A **Card Disabled Incident** incident is generated with Severity set to **Minor**.

**Note:** If the current card is a parent card, NNMi generates a **Card Disabled** incident on all daughter cards.

On the Source Object form, NNMi updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>CardDisabled</b> Conclusion.  <b>Note:</b> If the SNMP Agent reports the card has an Operational State of Down, then NNMi also adds a <b>CardDown</b> conclusion. The <b>Card Down</b> incident is not generated.
Incident	Adds the <b>Card Disabled</b> incident.  The <b>Correlated Children</b> tab includes any associated traps.
Status	Adds the <b>Disabled</b> Status.
Overall Status	Changes to <b>Disabled</b>


The Source Node map icon does not change color because this incident does not affect Node Status.

When NNMi determines that the card has an Administrative State of Up, NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "[Incident Form: General Tab](#)" on page 314 for more information.

See "[Card Form](#)" on page 157 for more information about card States and Status.

## Card Down

You receive a **Card Down** incident when NNMi analyzed the situation and determined any of the following:

- The card's **Operational State** is  **Down**.
- The Daughter card's **Operational State** is  **Down**.

A **Card Down** incident is generated with Severity set to **Critical**.

On the Source Object form, NNMi updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>CardDown</b> Conclusion.
Incident	Adds the <b>Card Down</b> incident.  The <b>Correlated Children</b> tab includes the following: <ul style="list-style-type: none"> <li>All <b>ConnectionDown</b> and <b>InterfaceDown</b> incidents that are associated with this card under this incident.</li> <li>Any associated traps.</li> </ul>
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

On the Source Node form, NNMi updates information on the following tabs:

### Source Node Updates

Tab	Description
Cards	Changes the State and Status of the cards hosted on the node that have an Operational State of Down to <b>Critical</b> .
Interfaces	Changes the State and Status of interfaces hosted on the card that have an Operational State of Down to <b>Critical</b> .
Status	Adds the <b>Minor</b> Status.
Conclusions	<b>CardsDownInNode</b>

On the maps, the icon for the Source Node is set to yellow.

When NNMi determines that the Card has an Operational State of Up, the Node can be reached, and all of the Node's IP addresses respond to ICMP, NNMi updates the following attributes:

- The Card Status is changed to **Normal**.
- The Card Conclusion is changed to CardUp.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See ["Incident Form: General Tab" on page 314](#) for more information.
- The Node Status is changed to **Normal**. The Conclusion on the Node is CardsUpInNode.

See ["Card Form" on page 157](#) for more information about card states and status.

## Card Undetermined State

**Note:** The **Card Undetermined State** incident is disabled by default. If you are an NNMi administrator, see [Generate Card Undetermined State Incidents](#) for information about how to enable this incident.

You receive a **Card Undetermined State** incident when NNMi cannot determine the Card's State for one of the following reasons:

- The SNMP agent responded with a value for the card's Operational Status of **Unavailable**
- The SNMP agent returned a value outside the range of possible values or returned a null value

A **Card Undetermined State** incident is generated with Severity set to **Minor**.

On the Source Object form, NNMi updates information on the following tabs:

#### Source Object Updates

Tab	Description
Conclusion	Adds the <b>CardUndeterminedState</b> Conclusion.
Incident	Adds the <b>Card Undetermined State</b> incident.
Status	Adds the <b>Minor</b> Status.
Overall Status	Changes to <b>Minor</b> .

On the Source Node form, NNMi updates information on the following tabs:

#### Source Node Updates

Tab	Description
Cards	Changes the State and Status of the cards hosted on the node that have a Status of Minor to <b>Minor</b> .
Status	Adds the <b>Minor</b> Status.
Conclusions	<b>CardsUndeterminedStateInNode</b>

On the maps, the icon for the Source Node is set to yellow.

When NNMi determines that the card has an Operational State of Up, NNMi updates the following attributes:

- The Card Status changes to **Normal**.
- The Card Conclusion changes to CardUp.
- NNMi updates Information in the Correlation Notes attribute and closes the incident. See ["Incident Form: General Tab" on page 314](#) for more information.

See ["Card Form" on page 157](#) for more information about card States and Status.

## 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**.

On the Source Object form, NNMi updates information on the following tabs:

### Source Object Updates

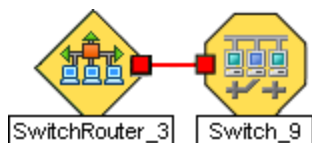
Tab	Description
Conclusion	Adds the <b>ConnectionDown</b> Conclusion.
Incident	Adds the <b>Connection Down</b> incident.
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .





On the Source Node form, NNMi updates information on the following tabs:

### Source Node Updates

Tab	Description
Interfaces	Changes the State and Status of interfaces hosted on the node that have an Operational State of Down to <b>Critical</b> .
Status	Adds the <b>Minor</b> Status.
Conclusions	<b>InterfacesDownInNode</b>

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.
-  Blue: due to other network problems, the status of one interface cannot be determined at this time.

When NNMi determines that the Connection is Up, NNMi updates the following attributes:

- The Connection Status is changed to **Normal**.
- The Connection Conclusion is changed to ConnectionUp.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.

## 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 Object form, NNMi updates information on the following tabs:

#### Source Object Updates

Tab	Description
Conclusion	Adds the <b>CpuOutOfRangeOrMalfunctioning</b> Conclusion.
Incident	Adds the <b>CPU Utilization is too High</b> incident. The <b>Correlated Children</b> tab includes any associated traps.
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

When NNMi determines that the CPU utilization is nominal, NNMi updates the following attributes:

- The Source Object Status is changed to **Normal**.
- The Source Object Conclusion is changed to **CpuInRangeAndFunctioning**.
- NNMi updates Information in the **Correlation Note** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.

## Custom Polled Instance in Collection is Out of Range

**Note:** The NNMi administrator determines whether NNMi generates **Custom Polled Instance**<sup>1</sup> incidents. If you are an NNMi administrator, see **Configure Basic Settings for a Custom Poller Collection** for more information.

A **Custom Polled Instance in Collection is Out of Range** incident indicates a Custom Polled Instance has reached or exceeded a Comparison Map value or Threshold configured for the associated **Custom Node Collection**<sup>2</sup>.

A **Custom Polled Instance in Collection is Out of Range** incident is generated with the Severity equal to the Status of the Custom Polled Instance. For example, if the Status of the

---

<sup>1</sup>A Custom Polled Instance represents the results of a MIB expression when it is evaluated against a node. The first time a MIB Expression is validated with discovery information, the results appear in the Monitoring workspace's Custom Polled Instances view. The Custom Polled Instance is updated whenever a change in State occurs and includes the most recent polled value that caused the State to change. These results are then used to determine the Status of the associated Custom Node Collection.

<sup>2</sup>A Custom Node Collection identifies a topology node that has at least one associated Custom Poller Policy. Because a topology node can be associated with more than one Policy, the same topology node might appear in multiple Custom Node Collections.

Custom Polled Instance is Critical, NNMi generates the associated incident with a Severity of Critical.

If the Status of the Custom Polled Instance is Normal, NNMi does not generate an incident.

The Name of the Source Object for a Custom Polled Instance Incident is the display value that is determined using the Instance Display Configuration for the associated MIB Expression.

If the Instance Display Configuration is not set, NNMi identifies the Source Object using the topology Node Name followed by the MIB Instance value in the format: `<node_name> -.<MIB_instance_value>`.

**Note:** The Name that NNMi uses to identify the Custom Polled Instance Incident's Source Object is not stored in the NNMi database as the Custom Polled Instance object Name.

On the Custom Polled Instance form, NNMi updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds one of the following Conclusions: CustomPolledInstanceCritical CustomPolledInstanceMajor CustomPolledInstanceMinor CustomPolledInstanceWarning
Incident	Adds the <b>Custom Polled Instance in Collection is Out of Range</b> incident.
Status	Adds the Status of the Custom Polled Instance object.
Overall Status	Changes to the Status of the Custom Polled Instance object.

When NNMi determines that the Custom Polled Instance is Normal, NNMi updates the following attributes:

- The Custom Polled Instance Status is changed to **Normal**.
- The Custom Polled Conclusion is changed to CustomPolledInstanceNormal.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See ["Incident Form: General Tab"](#) on page 314 for more information.

## Fan is Out of Range or Malfunctioning

A **Fan is Out of Range or Malfunctioning** incident indicates the identified fan on the Source Node is not operating correctly.

A **Fan is Out of Range or Malfunctioning** incident is generated with Severity set to **Critical**.

**Note:** Only the health of the Fan and Power Supply Node Components are propagated to the Node level.

On the Source Object form, NNMi updates information on the following tabs:



**Source Object Updates**

Tab	Description
Conclusion	Adds the <b>FanOutOfRangeOrMalfunctioning</b> Conclusion.
Incident	Adds the <b>Fan is Out of Range or Malfunctioning</b> incident. The <b>Correlated Children</b> tab includes any associated traps.
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

On the Source Node form, NNMi updates information on the following tabs:

**Source Node Updates**

Tab	Description
Node Components	The State and Status of malfunctioning fans that are hosted on the node are changed to <b>Critical</b> .
Status	Adds the <b>Major</b> Status.
Conclusions	<b>NodeWithBadFan</b>

On the map, the Causal Engine sets the color of the Source Node to orange.

When NNMi determines that the fan is functioning properly, NNMi updates the following attributes:

- The Node Component Status changes to **Normal**.
- The Node Component Conclusion changes to FanInRangeAndFunctioning.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See ["Incident Form: General Tab"](#) on page 314 for more information.
- The Conclusion on the Node is NodeWithGoodFans.

## 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**.

On the Source Object form, NNMi updates information on the following tabs:

**Source Object Updates**

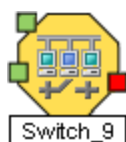
Tab	Description
Conclusion	Adds the <b>InterfaceDown</b> Conclusion.
Incident	Adds the <b>Interface Down</b> incident.
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

On the Source Node form, NNMi updates information on the following tabs:

### Source Node Updates

Tab	Description
Interfaces	Changes the State and Status of the interface to <b>Critical</b> . <b>Note:</b> You might find relevant traps on the <b>Correlated Children</b> tab.
Addresses	If the interface has one or more addresses, the State and Status is <b>Critical</b> if the address is no longer reachable.
Status	Adds the <b>Minor</b> Status.
Conclusions	<b>InterfacesDownInNode</b>

On the maps, the icons for the Source Node and its interfaces are updated:



When the Interface is operationally up, the Node can be reached, and all of the Node's IP Addresses respond to ping, NNMi updates the following attributes:

- The Interface Status is changed to **Normal**.
- The Interface Conclusion is changed to InterfaceUp.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See ["Incident Form: General Tab"](#) on page 314 for more information.
- The Node Status is changed to **Normal**. The Conclusion on the Node is `InterfaceUpInNode`.

## 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. If you are an NNMi administrator, see [Generate Interface Disabled Incidents](#) for information about how to enable this incident.

An **Interface Disabled** incident is generated with Severity set to **Critical**.

On the Source Object form, NNMi updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>InterfaceDisabled</b> Conclusion.
Incident	Adds the <b>Interface Disabled</b> incident.

**Source Object Updates, continued**

Tab	Description
	<p><b>Note:</b> If the SNMP agent reports that the Operational State of the interface is Down, an <b>InterfaceDown</b> Conclusion is also added. The <b>Interface Down</b> incident is not generated.</p> <p>The <b>Correlated Children</b> tab includes any associated link down traps.</p>
Status	Adds the <b>Disabled</b> Status.
Overall Status	Changes to <b>Disabled</b> .
Associated IP Addresses	Adds the <code>AddressDisabled</code> Conclusion.

On the maps, the icons for any of the Source Node's disabled interfaces are updated, the color of the interface icon changes to gray (disabled):



When the Interface is administratively up, the node's SNMP Agent is up, and the IP Address associated with the Interface responds to ICMP, NNMi updates the following attributes:

- The Interface Status is changed to **Normal**.
- The Interface Conclusion is changed to `InterfaceEnabled`.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "[Incident Form: General Tab](#)" on page 314 for more information.
- The Interface's IP Addresses Status is changed to **Enabled**. The Conclusion on the IP Address is `AddressEnabled`.

## IP Subnet Contains IP with New MAC Address

NNMi generates an **IP Subnet Contains IP with New MAC Address** when it detects that the MAC Address corresponding to a particular IP Address has changed. This situation might occur when NNMi performs a configuration poll on certain devices (for example, routers) and indicates that a possible duplicate IP Address exists on this subnet.

**Note:** NNMi can detect a change in the MAC address even if the particular IP Address is not discovered.

An **IP Subnet Contains IP with New MAC Address** incident is generated with Severity set to **Major**.

The Source Node map icon does not change color because this incident does not affect Node Status.

After 24 hours, NNMi automatically closes the incident.

## 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 Object form, NNMi updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>MemoryOutOfRangeOrMalfunctioning</b> Conclusion.
Incident	Adds the <b>Memory has Insufficient Capacity or is Malfunctioning</b> incident. The <b>Correlated Children</b> tab includes any associated traps.
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

On the Source Node form, NNMi updates information on the following tabs:

### Source Node Updates

Tab	Description
Node Components	Changes the State and Status of the malfunctioning memory to <b>Critical</b> .
Status	Adds the <b>Major</b> Status.
Conclusions	<b>NodeWithBadMemory</b>

On the map, the Causal Engine sets the color of the Source Node to yellow.

When NNMi determines that the memory pool is functioning properly, NNMi updates the following attributes:

- The Source Object Status is changed to **Normal**.
- The Source Object Conclusion is changed to **MemoryInRangeAndFunctioning**.
- NNMi updates Information in the Correlation Notes attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.
- The Source Node Conclusion is changed to **NodeWithGoodMemory**.

## 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.
- A node that has no discovered connections is unreachable. (No connections have been discovered for the node.)
- 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 node's neighbor is up and the node is unresponsive.

Reasons NNMi might not successfully 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 gathers only the address information for the node.

A Node Down incident is generated with Severity set to **Critical**, and the map icon is set to red (see [Map Displays](#)).

On the Source Object form, NNMi updates information on the following tabs:

**Source Object Updates**

Tab	Description
Conclusion	Adds the <b>NodeDown</b> Conclusion.
Incident	Adds the <b>Node Down</b> incident.  On the <b>Correlated Children</b> tab, any <b>Interface Down</b> incident on neighbors that are one hop from the node are correlated under the <b>Node Down</b> incident.
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

**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 the next page for more information.

NNMi does not generate a Node Down incident for node under the following conditions:

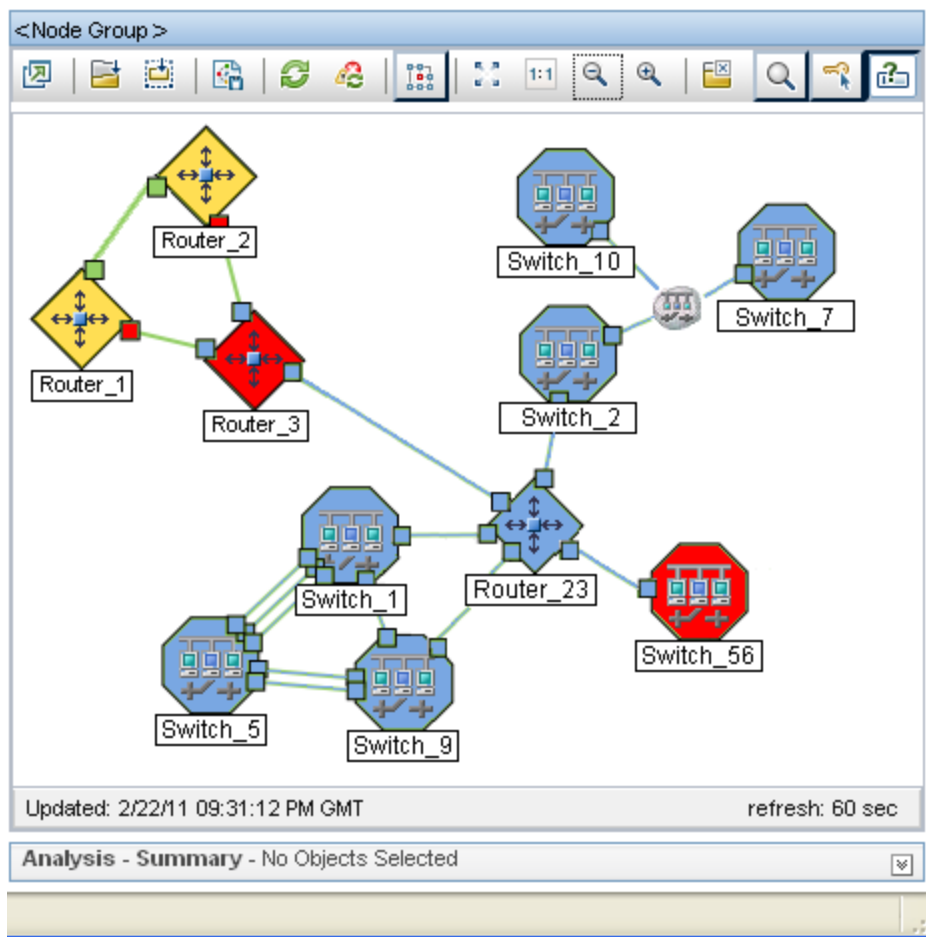
- If the node is in the shadow of another node that causes the node to be unreachable.
- If the node is in an ATM or Frame Relay cloud that causes the node to be unreachable.

**Map Displays**

The Status of the Node Down device for a Source 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.
- Nodes that are members of the Important Nodes group's map icons change to red (Switch\_56 in the illustration below).



When NNMi determines that the Node is Up, NNMi updates the following attributes:

- The Node Status is changed to **Normal**.

**Note:** If all of the access switches to any Nodes in the shadow are reachable, the Status of any Nodes in the shadow is also changed to **Normal**.

- The Node Conclusion is changed to NodeUp.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.

## Node or Connection Down

If a non-SNMP node is not responding to ICMP or an SNMP 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 Object form, NNMi updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>NodeOrConnectionDown</b> Conclusion.
Incident	Adds the <b>Node or Connection Down</b> incident.  On the <b>Correlated Children</b> tab, the Interface Down incident on neighbor that is one hop from the node is correlated under the <b>Node or Connection Down</b> incident.
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

### Map Displays

The Status of the Node or Connection Down device for a Source Node changes to **Critical** and the device's map icon color changes to red .

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.
- Nodes that are members of the Important Nodes group's map icons change to red.

**Tip:** See "Map Displays" in "Node Down" on page 404 for more information.

When NNMi determines that the Source Node in the Connection is Up, NNMi updates the following attributes:

- The Node Status is changed to **Normal**.
- The Connection Status is changed to **Normal**.
- The Node Conclusion is changed to NodeUp.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.

## Power Supply is Out of Range or 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**.

**Note:** Only the health of the Power Supply and Fan Node Components are propagated to the Node level.

On the Source Object form NNMi updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>PowerSupplyOutOfRangeOrMalfunctioning</b> Conclusion.
Incident	Adds the <b>Power Supply is Malfunctioning</b> incident. The <b>Correlated Children</b> tab includes any associated traps.
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

On the Source Node form, NNMi updates information on the following tabs:

### Source Node Updates

Tab	Description
Node Components	Changes the State and Status of the malfunctioning fan to <b>Critical</b> .
Status	Adds the <b>Major</b> Status.
Conclusions	<b>NodeWithBadPowerSupply</b>

On the map, the Causal Engine sets the color of the Source Node to orange.

When NNMi determines that the power supply is functioning properly, NNMi updates the following attributes:

- The Source Object Status is changed to **Normal**.
- The Source Object Conclusion is changed to PowerSupplyInRangeAndFunctioning.
- NNMi updates Information in the Correlation Notes attribute and closes the incident. See ["Incident Form: General Tab"](#) on page 314 for more information.
- The Source Node Conclusion is NodeWithGoodPowerSupply.

## Island Group Down

A **Island Group Down** incident is generated when all of the nodes in an Island do not respond to ICMP or SNMP queries.

An Island Group is a group of fully-connected nodes discovered by NNMi, and NNMi determines this group is not connected to the rest of the topology.

**Note:** Islands must have at least two nodes, are created by NNMi, and cannot be modified.

An example of an environment with multiple Islands 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 checks for Islands and, when applicable, automatically creates them whenever it detects changes in Layer 2 Connections.

NNMi selects a representative node in each Island as the Source Node associated with the Island Group Down incident. The Source Object for this incident is the Island Group.

When NNMi determines that a node in the Island is reachable, NNMi updates the information in the **Correlation Notes** attribute and closes the incident. See "[Incident Form: General Tab](#)" on page 314 for more information.

## SNMP Agent Not Responding

NNMi periodically uses SNMP to check the availability of each SNMP Agent in your network environment. Possible reasons an SNMP Agent is not responding include the following:

- The SNMPv1 or SNMPv2c *read community string* for this agent changed
- The SNMPv3 User Name for this agent changed and the NNMi communication configuration settings have not yet been updated

A **SNMP Agent Not Responding** incident is generated with Severity set to **Minor**.

On the Source Object form, NNMi updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>SNMPAgentNotResponding</b> Conclusion.
Incident	Adds the <b>SNMP Agent Not Responding</b> incident.
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

On the Source Node form, NNMi updates information on the following tabs:

### Source Node Updates

Tab	Description
Interfaces	The Status of polled interfaces is set to <b>Unknown</b> .
Status	Adds the <b>Minor</b> Status.
Conclusions	<b>UnresponsiveAgentInNode</b>

On the maps, the icons for the monitored Source Node (status = Minor) and its interfaces (status = **Unknown**) are updated:



When NNMi determines that the agent is responding, NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.

When NNMi determines that SNMP Agent for the Source Node is responding, NNMi updates the following attributes:

- The SNMP Agent Status is changed to **Normal**.
- The SNMP Agent Conclusion is changed to **SNMPAgentResponding**.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.
- The Node Status is changed to **Normal**. The Conclusion on the Node is **ResponsiveAgentInNode**.
- The Node's Interfaces return to their previous Status and the **InterfaceUnmanageable Conclusion** is cleared from the Node's polled Interfaces.
- The Node's Cards return to their previous Status and the **CardUnmanageable Conclusion** is cleared from the Node's polled Cards.

## SNMP Agent Ping Not Responding

NNMi periodically performs ICMP requests to the SNMP Agent IP Address. If there is no response and the node is not completely unreachable, NNMi's Causal Engine determines that the SNMP Agent IP Address on the device is not responding.

On the Source Object form NNMi updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>SNMPAgentPingNotResponding</b> Conclusion.
Incident	No incident is generated. The <b>Correlated Children</b> tab includes any associated traps.
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

On the Source Node form, NNMi updates information on the following tabs:

### Source Node Updates

Tab	Description
Status	Adds the <b>Minor</b> Status.
Conclusions	<b>SNMPAgentPingUnresponsiveInNode</b>

On the maps, the icon for the Source Node is set to yellow.

When the SNMP Agent IP Address starts responding to ICMP requests, NNMi updates the following attributes:

- The SNMP Agent IP Address Status is changed to **Normal**.
- The SNMP Agent IP Address Conclusion is changed to SNMPAgentPingResponding.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.
- The Source Node Conclusion is SNMPAgentPingResponsiveInNode.

## 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 Object form, NNMi updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>TemperatureOutOfRangeOrMalfunctioning</b> Conclusion.
Incident	Adds the <b>Temperature Sensor is Out of Range</b> incident. The <b>Correlated Children</b> tab includes any associated traps.
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

The Source Node map icon does not change color because this incident does not affect Node Status.

When NNMi determines that the temperature sensor is within the normal range (nominal), NNMi updates the following attributes:

- The Node Status changes to **Normal**.
- The Node Conclusion changes to TemperatureInRangeAndFunctioning.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.

## 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 Object form, NNMi updates information on the following tabs:

**Source Object Updates**

Tab	Description
Conclusion	Adds the <b>VoltageOutOfRangeOrMalfunctioning</b> Conclusion.
Incident	Adds the <b>Voltage is Out of Range</b> incident. The <b>Correlated Children</b> tab includes any associated traps.
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b>

The Source Node map icon does not change color because this incident does not affect Node Status.

When NNMi determines that the voltage is within the normal range (nominal), NNMi updates the following attributes:

- The Node Component Status changes to **Normal**.
- The Node Component Conclusion changes to **VoltageInRangeAndFunctioning**.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.

## Interpret Incidents Related to SNMP Traps

**Tip:** Also see "Investigate and Diagnose Problems" on page 355 for more information about troubleshooting tools that NNMi provides.

In addition to tracking Root Cause Incidents, NNMi accepts traps and (if there is a corresponding incident configuration that is enabled) generates a corresponding incidents to inform you of a potential problem.

The following incidents are generated as a result of exceeding SNMP trap threshold or queue size limits.

- "Hosted Object Trap Storm" on the next page
- "Pipeline Queue Size Exceeded " on page 415
- "SNMP Trap Limit (Warning, Major or Critical)" on page 416
- "Trap Storm" on page 417

**Note:** If you are an NNMi administrator, see [Control which Incoming Traps Are Visible in Incident Views](#) for a list of the SNMP Trap Incidents that NNMi enables by default.

(*NNMi Advanced*) The following Incidents are generated only in a Global Network Management Environment:

- "Message Queue Incident Rate Exceeded (NNMi Advanced)" on page 414
- "Message Queue Size Exceeded (NNMi Advanced)" on page 415

## Hosted Object Trap Storm

A **Hosted Object Trap Storm** incident indicates that the trap rate for an object on the specified node has exceeded a configured threshold.

**Tip:** The NNMi administrator can control traffic from traps with thresholds and blocking:

- [nnmtrapconfig.ovpl](#)
- [hosted-object-trapstorm.conf](#)

Use this incident to determine the following:

### Trap Information Source

CIA	Description
trapSource	The IP address of the SNMP agent from which the SNMP traps originated.
totalTrapRate	The total trap rate for the Node identified as the Source Node.
Suppressed Hosted Objects	<p>A report containing all of the Source Objects on the specified Node that have exceeded a trap rate threshold. All SNMP traps are suppressed for the specified Object when the trap rate threshold is exceeded.</p> <p>Note the following:</p> <ul style="list-style-type: none"><li>• The report tracks the average trap rate over time.</li></ul> <p><b>Tip:</b> If a trap storm spike was the source of the problem, this report might show a lower than expected trap rate, because NNMi gathers the report data after the initial incident.</p> <ul style="list-style-type: none"><li>• If the report exceeds the 2000 character limit, NNMi continues to log the information using subsequent files numbered consecutively; for example: <code>suppressedHosteObjects.1</code>, <code>suppressedHostedObjects.2</code>, and so on.</li></ul>
Unsuppressed Hosted Objects	<p>A report containing all of the Source Objects on the specified Node that have traps that are not currently suppressed. This means the trap rate threshold has not been exceeded for these objects.</p> <p>Note the following:</p> <ul style="list-style-type: none"><li>• The report tracks the average trap rate over time.</li></ul> <p><b>Tip:</b> If a trap storm spike was the source of the problem, this report might show a lower than expected trap rate, because NNMi gathers the report data after the initial incident.</p> <ul style="list-style-type: none"><li>• If the report exceeds the 2000 character limit, NNMi continues to log the information using subsequent CIAs numbered consecutively; for example: <code>unsuppressedHosteObjects.1</code>, <code>unsuppressedHostedObjects.2</code>, and so on.</li></ul>

Note the following:

- By default NNMi determines threshold rates every 2 minutes. This means a trap rate must be below the threshold for at least the 2 minute interval before the incident is canceled.
- If multiple objects are exceeding the specified threshold, NNMi generates the incident as soon as one object exceeds the configured threshold. The Source Object for the incident is the first object that exceeds the trap storm threshold.

On the maps, the icon for the Source Node is set to teal.

When the trap rate returns to below the configured threshold, NNMi cancels the incident.

See "Incident Form: General Tab" on page 314 for more information.

## Message Queue Incident Rate Exceeded (NNMi Advanced)

(NNMi Advanced) This incident applies to NNMi's Global Network Management feature, see "NNMi's Global Network Management Feature (NNMi Advanced)" on page 21 for more information about this feature.

**Note:** A queue is established on each Regional Manager. This queue holds information to be forwarded to the Global Manager.

A **Message Queue Incident Rate Exceeded** incident indicates that the volume of messages entering a Regional Manager's Global Network Management message queue has exceeded rate limits: 20 incidents per second within a 5 minute period (6,000 incidents within 5 minutes). NNMi would generate this Incident if a sudden burst of incident forwarding occurs (for example, 6,001 incidents within 2 minutes).

When the message queue's incident rate High limit is crossed, NNMi does the following:

- Generates a **Message Queue Incident Rate Exceeded** incident with the Severity set to **Critical**.
- Generates a **GlobalNetworkManagementIncidentRateLimitExceeded** health conclusion with the Severity set to **Major**.
- Stops forwarding to Global Managers any incidents generated from SNMP Traps and NNM 6.x/7.x Remote Events.

**Note:** The NNMi administrator must specifically configure SNMP Traps and NNM 6.x/7.x Remote Events to be forwarded from this Regional Manager to Global Managers.

**Tip:** To view the associated conclusion information, check the health of the Regional Manager using the **Health** tab from **Help** → **System Information**.

NNMi closes the incident when the incident rate falls below 90 percent of the incident rate limit and the next incident has been successfully forwarded.

## Message Queue Size Exceeded (NNMi Advanced)

(*NNMi Advanced*) When the Global Network Management feature is enabled, a queue is established on each Regional Manager. This queue holds information to be forwarded to Global Managers. See "["NNMi's Global Network Management Feature \(NNMi Advanced\)"](#) on page 21 for more information about this feature.

A **Message Queue Size Exceeded** incident indicates that a Regional Manager's Global Network Management message queue has exceeded configured limits:

- Default lower limit is 200,000 messages.
- Default upper limit is 250,000 messages.

When the message queue size's lower limit is reached, NNMi generates the following:

- A **Message Queue Size Exceeded** incident with the Severity set to **Warning**.
- A **GlobalNetworkManagementIncidentQueueSizeLimit** health conclusion with the Severity set to **Warning**.

When the message queue size's upper limit is reached, NNMi generates the following:

- A **Message Queue Size Exceeded** incident with the Severity set to **Critical**.
- A **GlobalNetworkManagementIncidentQueueSizeLimit** health conclusion with the Severity set to **Major**.
- Stops forwarding to Global Managers any incidents generated from SNMP Traps and NNM 6.x/7.x Remote Events.

**Note:** The NNMi administrator must specifically configure SNMP Traps and NNM 6.x/7.x Remote Events to be forwarded from this Regional Manager to Global Managers.

**Tip:** To view the conclusion information that generated this incident, check the health of the Regional Manager using the **Health** tab from **Help** → **System Information**.

This incident indicates a connection problem with a Global Manager. Click **Help** → **System Information** and select the **Global Network Management** tab to identify which Global Manager is not currently connected.

To resolve this issue, communication with that Global Manager must be reestablished.

## Pipeline Queue Size Exceeded

A **Pipeline Queue Size Exceeded** incident indicates one of the queues connecting the stages for the Event Pipeline is above the configured limits. NNMi determines queue size limits based on memory size. Click [here](#) for more information about the Event Pipeline.

Any incident information that appears in your incident views first travels through the Event Pipeline. The Event Pipeline guarantees that the incident data is analyzed in chronological order.

**Note:** Not all information that travels through the pipeline results in an incident.

If at any time an incident does not meet the criteria for a stage in the Event Pipeline, it is ignored and passed to the next stage in the pipeline or it is dropped. For information about each of the stages in the Event Pipeline, see [Help for Administrators](#).

When the lower queue size limit is reached, NNMi generates the following:

- A **Pipeline Queue Size Exceeded** incident with the Severity set to **Major**.
- A **PipelineQueueSizeLowerLimitExceeded** health conclusion with the Severity set to **Major**.

**Tip:** To view the conclusion information that generated this incident, check the health of the Regional Manager using the **Health** tab from **Help** → **System Information**.

When the upper limit is reached, NNMi does the following:

- Generates a **Pipeline Queue Size Exceeded** incident with the Severity set to **Critical**.
- Generates a **PipelineQueueSizeHigherLimitExceeded** health conclusion with the Severity set to **Major**.

**Tip:** To view the associated conclusion information, check the health of the Regional Manager using the **Health** tab from **Help** → **System Information**.

- Drops incidents created from SNMP traps or Remote NNM 6.x/7.x Events, but continues to generate incidents created from Management Events.

To reduce the number of incidents in the queue, ask your NNMi administrator to disable any SNMP Trap or Remote NNM 6.x/7.x Event configurations that are not essential.

## SNMP Trap Limit (Warning, Major or Critical)

An **SNMP Trap Limit (Warning, Major or Critical)** incident indicates the number of SNMP traps has reached or exceeded the maximum limit. 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. If you are an NNMi administrator, see "Configuring the Auto-Trim Oldest SNMP Trap Incidents Feature" in the HP Network Node Manager i Software Deployment Reference for more information.

An **SNMP Trap Limit (Warning, Major or Critical)** incident is generated with Severity set to either **Warning**, **Major** or **Critical**.

When the number of traps reaches 90 percent of the maximum limit, NNMi generates the following:

- An **SNMP Trap Limit Warning** SNMP Trap incident with a Severity set to **Warning**.
- A health conclusion **SnmptTrapLimitExceeded** with the **Severity** set to **Warning**.

When the number of traps reaches 95 percent of this maximum limit, NNMi generates the following:

- An **SNMP Trap Limit Major** SNMP Trap incident with a Severity set to **Major**.
- A health conclusion **SnmptTrapLimitExceeded** with the **Severity** set to **Major**.

When the number of traps reaches the maximum limit, NNMi generates the following:

- An **SNMP Trap Limit Critical** SNMP Trap incident with a Severity set to **Critical**.
- A health conclusion **SnmptTrapLimitExceeded** with the **Severity** set to **Critical**.

**Tip:** To view the associated conclusion information, check the health of the NNMi management server using the **Health** tab from **Help** → **System Information**.



## Trap Storm

**Tip:** The NNMi administrator can control traffic from traps with thresholds and blocking:

- [nnmtrapconfig.ovpl](#)
- [hosted-object-trapstorm.conf](#)

A **Trap Storm** incident indicates one of the following:

- The *overall* trap rate in your network management domain exceeds a set threshold. Use the `overallThresholdRate` argument to the `nnmtrapconfig.ovpl` command to set this threshold.  
**Note:** The incident's `blockedSources` and `blockedTraps` CIA values are set to `all`.
- The trap rate on an IP address in a Node exceeds a set threshold. Use the `thresholdRate` argument to the `nnmtrapconfig.ovpl` command to set this threshold.  
**Note:** The incident's `blockedSources` CIA value contains the IP address of the node that is the source of the trap storm. The `blockedTraps` CIA is set to `all`.
- The overall trap rate for a specific trap (Object Identifier) exceeds a threshold. Use the `thresholdRate` argument to the `nnmtrapconfig.ovpl` command to set set this threshold.  
**Note:** The incident's `blockedSources` CIA value is set to `all`. The incident's `blockedTraps` CIA contains the Object Identifier (OID) of the trap that has exceeded the specified threshold value.

Note the following:

- NNMi determines threshold rates every 5 minutes. This means a trap rate must be below the threshold for at least the 5 minute interval before the incident is canceled.
- If multiple nodes are exceeding the specified threshold, NNMi tracks information for only the first node that has exceeded the trap storm threshold until it can cancel the incident.

Use this incident to determine the following:

### Trap Information Source

CIA	Description
trapRate	The trap rate for the first trap that has exceeded the threshold limit.
blockedSources	The IP address for the Node, if any, that has suppressed traps. <b>Note:</b> This CIA value is <code>all</code> if the overall trap rate is exceeded or if the overall trap rate for a specific trap OID is exceeded.
blockedTraps	A report containing all of the nodes that have traps that are currently suppressed. <b>Note:</b> This CIA value is <code>all</code> if the overall trap rate is exceeded or if the overall trap rate for a specific node is exceeded.

On the maps, the icon for the Source Node is set to teal.

When the trap rate returns to below the configured threshold, NNMI cancels the incident. See "Incident Form: General Tab" on page 314 for more information.

## Interpret Informational Incidents

**Tip:** Also see "Investigate and Diagnose Problems" on page 355 for more information about troubleshooting tools that NNMI provides.

In addition to tracking Root Cause Incidents, NNMI's Causal Engine tracks changes in your network and generates incidents to inform you of changes to your network devices that might be of interest. These incidents are informational and have a Correlation Nature of **Info**. To view these incidents, create a filter for the **All Incidents** view, using the Correlation Nature column, and select the value **Info** from the enumerated list of values. See [Filter a Table Views](#) for more information about using filters in table views.

Examples of incidents generated to inform you of network changes include the following:

- "Card Removed" below
- "Card Inserted" below

### Card Removed

**Tip:** Also see "Investigate and Diagnose Problems" on page 355 for more information about troubleshooting tools that NNMI provides.

A **Card Removed** incident indicates a card has been removed from the Source Node.

A **Card Removed** Incident is generated with the Severity set to **Warning**.

On the Source Object (which is a node) form, NNMI updates information on the following tab:

#### Source Node Updates

Tab	Description
Incident	Adds the <b>Card Removed</b> incident. The Correlated Children tab includes any associated traps.

**Note:** NNMI does not automatically close **Card Removed** incidents.

See "Card Form" on page 157 for more information about card States and Status.

### Card Inserted

**Tip:** Also see "Investigate and Diagnose Problems" on page 355 for more information about troubleshooting tools that NNMI provides.

A **Card Inserted** incident indicates a Card has been inserted into the Source Node.

A **Card Inserted** Incident is generated with the Severity set to **Normal**.

On the Source Object (which is a node) form, NNMI updates information on the following tab:

**Source Node Updates**

Tab	Description
Incident	Adds the <b>Card Inserted</b> incident. The Correlated Children tab includes any associated traps.

**Note:** NNMi does not automatically close **Card Inserted** incidents.

## Node Deleted

**Tip:** Also see "Investigate and Diagnose Problems" on page 355 for more information about troubleshooting tools that NNMi provides.

A **Node Deleted** incident indicates a Node was deleted from the NNMi topology.

A **Node Deleted** Incident is generated with the Severity set to **Normal**.

**Note:** NNMi does not automatically close **Node Deleted** incidents.

## 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.

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 that have a Correlation Nature of Service Impact:

- "Multiple Primary Cards in Card Redundancy Group" on the next page
- "Multiple Primary Devices in Router Redundancy Group (NNMi Advanced)" on page 421
- "Multiple Secondary Devices in Router Redundancy Group (NNMi Advanced)" on page 421
- "No Primary Card in Card Redundancy Group" on page 422
- "No Primary Device in Router Redundancy Group (NNMi Advanced)" on page 423
- "No Secondary Card in Card Redundancy Group" on page 424
- "No Secondary Device in Router Redundancy Group (NNMi Advanced)" on page 425

- "Primary Device in Router Redundancy Group Switched (NNMi Advanced)" on page 426
- "Router Redundancy Group Degraded (NNMi Advanced)" on page 426

**Note:** NNMi determines the Correlation Nature for an incident.

See "Router Redundancy Group View (NNMi Advanced)" on page 281 for more information about Router Redundancy Groups.

## Multiple Primary Cards in Card Redundancy Group

A **Multiple Primary Cards in Card Redundancy Group** incident means NNMi determined multiple primary cards (for example, Card Active) are identified in a Card Redundancy Group.

This incident typically indicates that communication between cards in the group is malfunctioning.

A **Multiple Primary Cards in Card Redundancy Group** incident has Severity set to **Critical**.

On the Source Object form, NNMi updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>CrgMultiplePrimary</b> Conclusion.
Incident	Adds the <b>Multiple Primary Cards in Card Redundancy Group</b> incident. The <b>Correlated Children</b> tab includes any associated traps. <b>Note:</b> If any cards in the group have an Operational State of Down, the <b>Card Down</b> incidents are correlated under the new incident
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

On the Source Node form, NNMi updates information on the following tabs:

### Source Node Updates

Tab	Description
Status	Adds the <b>Warning</b> Status.
Conclusions	<b>CrgMalfunctionInNode</b>

On the maps, the icon for the Source Node is set to teal.

When NNMi determines that the group contains one primary card, NNMi updates the following attributes:

- The Card Redundancy Group Status changes to **Normal**.
- The Card Redundancy Group Conclusion changes to CrgNormal.

- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.
- The Node Conclusion is CrgNormalInNode.

## Multiple Primary Devices in Router Redundancy Group (NNMi Advanced)

A **Multiple Primary Devices in Router Redundancy Group** incident means NNMi detected multiple primary devices in a Router Redundancy Group (for example, HSRP Active or VRRP Master).

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**.

On the Source Object form, NNMi updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>RrgMultiplePrimary</b> Conclusion.
Incident	Adds the <b>Multiple Primary Devices in Router Redundancy Group</b> incident. The <b>Correlated Children</b> tab includes any associated traps.
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

When NNMi detects that the group has one primary member, NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.

When NNMi determines that the group has one primary member, NNMi updates the following attributes:

- The Router Redundancy Group Status changes to **Normal**.
- The Router Redundancy Group Conclusion changes to RrgOnePrimary.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.

## Multiple Secondary Devices in Router Redundancy Group (NNMi Advanced)

A **Multiple Secondary Devices in Router Redundancy Group** incident means NNMi detected more than one secondary router in a Router Redundancy Group using a Router Redundancy Protocol that does not allow more than one router in a secondary role. That Router Redundancy

Protocol has a third designator to indicate routers that are available, but not currently serving as primary or secondary (for example, HSRP Listen).

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**.

On the Source Object form NNMi updates information on the following tabs:

**Source Object Updates**

Tab	Description
Conclusion	Adds the <b>RrgMultipleSecondary</b> Conclusion.
Incident	Adds the <b>Multiple Secondary Devices in Router Redundancy Group</b> incident.  The <b>Correlated Children</b> tab includes any associated traps.
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

When NNMi determines that the group has has one secondary member, NNMi closes the incident and changes the Router Redundancy Group Status to **Normal**. No Conclusion is added.

## No Primary Card in Card Redundancy Group

A **No Primary Card in Card Redundancy Group** incident means NNMi determined no primary card (for example, Card Active) is identified in a Card Redundancy Group.

This typically indicates one of the following:

- One card, or both cards have an Operational State of Down
- NNMi has identified only secondary cards (for example Card Standby) in the Card Redundancy Group
- Communication between cards in the Card Redundancy Group is malfunctioning

A **No Primary Card in Card Redundancy Group** incident has Severity set to **Critical**.

On the Source Object form, NNMi updates information on the following tabs:

**Source Object Updates**

Tab	Description
Conclusion	Adds the <b>CrgNoPrimary</b> Conclusion.
Incident	Adds the <b>No Primary Card in Card Redundancy Group</b> incident.  The <b>Correlated Children</b> tab includes any associated traps  <b>Note:</b> If there are cards down in the group, the <b>Card Down</b> incidents is correlated

### Source Object Updates, continued

Tab	Description
	under the new incident
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

On the Source Node form, NNMi updates information on the following tabs:

### Source Node Updates

Tab	Description
Status	Adds the <b>Warning</b> Status.
Conclusions	<b>CrgMalfunctionInNode</b>

On the maps, the icon for the Source Node is set to teal.

When NNMi determines that the group contains a primary card, NNMi updates the following attributes:

- The Card Redundancy Group Status changes to **Normal**.
- The Card Redundancy Group Conclusion changes to CrgNormal.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.
- The Node Conclusion is CrgNormalInNode.
- 

## No Primary Device in Router Redundancy Group (NNMi Advanced)

A **No Primary Device in Router Redundancy Group** incident means NNMi detected zero primary devices in a Router Redundancy group (for example, zero HSRP Active or VRRP Master).

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**.

On the Source Object form, NNMi updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>RrgNoPrimary</b> Conclusion.

**Source Object Updates, continued**

Tab	Description
Incident	Adds the <b>No Primary Device in Router Redundancy Group</b> incident. The <b>Correlated Children</b> tab includes any associated traps. <b>Note:</b> If an interface in the group has an Operational State of Down, its <b>Interface Down</b> incident is correlated under this incident.
Status	Adds the <b>Critical</b> Status.
Overall Status	Changes to <b>Critical</b> .

When NNMi determines that the group NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "[Incident Form: General Tab](#)" on page 314 for more information.

When NNMi determines that the group has a Primary member, NNMi updates the following attributes:

- The Router Redundancy Group Status changes to **Normal**.
- The Router Redundancy Group Conclusion changes to RrgOnePrimary.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "[Incident Form: General Tab](#)" on page 314 for more information.

## No Secondary Card in Card Redundancy Group

A **No Secondary Card in Card Redundancy Group** incident means NNMi determined no secondary card (for example, Card Standby) is identified in a Card Redundancy Group.

This typically indicates the following:

- One of the two cards in the group has an Operational State of Down.
- The other card has been identified as primary (for example, Card Active).
- The Card Redundancy Group is functioning properly.

A **No Primary Card in Card Redundancy Group** incident has Severity set to **Minor**.

On the Source Object form, NNMi updates information on the following tabs:

**Source Object Updates**

Tab	Description
Conclusion	Adds the <b>CrgNoSecondary</b> Conclusion.
Incident	Adds the <b>No Secondary Card in Card Redundancy Group</b> incident. The <b>Correlated Children</b> tab includes any associated traps <b>Note:</b> If there are cards down in the group, the <b>CardDown</b> incidents is correlated under the new incident



### Source Object Updates, continued

Tab	Description
Status	Adds the <b>Minor</b> Status.
Overall Status	Changes to <b>Minor</b> .

On the Source Node form, NNMi updates information on the following tabs:

### Source Node Updates

Tab	Description
Status	Adds the <b>Warning</b> Status.
Conclusions	<b>CrgMalfunctionInNode</b>

On the maps, the icon for the Source Node is set to teal.

When NNMi determines that the group contains a secondary card, NNMi updates the following attributes:

- The Card Redundancy Group Status changes to **Normal**.
- The Card Redundancy Group Conclusion changes to CrgNormal.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 314 for more information.
- The Node Conclusion is CrgNormalInNode.

## No Secondary Device in Router Redundancy Group (NNMi Advanced)

A **No Secondary Device in Router Redundancy Group** incident means NNMi detected zero secondary devices in a Router Redundancy Group (for example, zero HSRP Standby or VRRP Backup).

This incident typically indicates the following:

- Protocol-specific communication between routers in the group is malfunctioning.
- The group is routing packets properly because NNMi detected a primary device.

A **No Secondary Device in Router Redundancy Group** incident has Severity set to **Warning**.

On the Source Object form, NNMi updates information on the following tabs:

### Source Object Updates

Tab	Description
Conclusion	Adds the <b>RrgNoSecondary</b> Conclusion.
Incident	Adds the <b>No Secondary Device in Router Redundancy Group</b> incident.

### Source Object Updates, continued

Tab	Description
	The <b>Correlated Children</b> tab includes any associated traps. <b>Note:</b> If an interface in the group has an Operational State of Down, its <b>Interface Down</b> incident is correlated under this incident.
Status	Adds the <b>Warning</b> Status.
Overall Status	Changes to <b>Warning</b> .

When NNMi determines that the group has a secondary member, NNMi closes the incident and changes the Router Redundancy Group Status to **Normal**. No Conclusion is added.

## Primary Device in Router Redundancy Group Switched (*NNMi Advanced*)

A **Primary Device in Router Redundancy Group Switched** incident means NNMi detected that the Primary role 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**

On the Source Object form, NNMi updates information on the following tab:.

### Source Object Updates

Tab	Description
Incident	Adds the <b>Primary Device in Router Redundancy Group Switched</b> incident. The <b>Correlated Children</b> tab includes any associated traps.

## Router Redundancy Group Degraded (*NNMi Advanced*)

This incident occurs only in Router Redundancy Groups with more than two routers.

A **Router Redundancy Group Degraded** incident means NNMi determined the following:

- The Router Redundancy Group still has a primary and secondary device.
- The remaining devices in the group are down or in an unexpected protocol-specific state. For example, in HSRP other member routers should be in Listen state.

Typically, the protocol-specific communication between routers is malfunctioning. However, the group is routing packets properly.

A **Router Redundancy Group Degraded** incident has Severity set to **Warning**.

On the Source Object form, NNMi updates information on the following tabs:

**Source Object Updates**

Tab	Description
Conclusion	Adds the Conclusion RrgDegraded.
Incident	Adds the <b>Router Redundancy Group Degraded</b> incident. The <b>Correlated Children</b> tab includes any associated traps. <b>Note:</b> If an interface in the group has an Operational State of Down, the <b>Interface Down</b> incidents are correlated under this incident.
Status	Adds the <b>Warning</b> Status.
Overall Status	Changes to <b>Warning</b> .

When NNMi determines that the group has a active, standby and listen members, NNMi closes the incident and changes the Router Redundancy Group Status to **Normal**. No Conclusion is added.

## Interpret Threshold Incidents

The following tables describe some of the thresholds for which the NNMi administrator can enable incidents. For more information:

**Fault Threshold Threshold Incidents**

Threshold Being Monitored	Incidents
Management Address ICMP Response Time Threshold based on elapsed time (in milliseconds) for receiving a node's reply to an Internet Control Message Protocol (ICMP) echo request. The address queried is the node's Management Address attribute value. See the node's <a href="#">Node form, Basic Attributes section</a> for the currently configured address.	See "Management Address ICMP Response Time Incidents " on page 445

(*NNM iSPI Performance for Metrics*) 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 that have interfaces outside one or more threshold boundaries.

**Performance Threshold Incidents (NNM iSPI Performance for Metrics)**

Threshold Being Monitored	Incidents
<p>Backplane Utilization</p> <p>Threshold based on the percentage of backplane usage compared to the total amount of available backplane resources.</p>	<p>See "Backplane Incidents (NNM iSPI Performance for Metrics)" on page 431</p>
<p>Buffer monitoring:</p> <ul style="list-style-type: none"> <li>• Buffer Failure Rate                     <p>Threshold based on the percentage of a node's buffer failures compared to the total number of attempts to create new buffers. These failures are caused by insufficient memory when the device tried to create new buffers.</p> </li> <li>• Buffer Miss Rate                     <p>Threshold based on the percentage of a Node's buffer misses compared to the total attempts at buffer access. Crossing this threshold indicates the number of available buffers are dropping below a minimum level required for successful operation.</p> </li> <li>• Buffer Utilization                     <p>Threshold based on the percentage of a Node's buffers that are currently in use, compared to the total number of available buffers.</p> </li> </ul>	<p>See "Buffer Incidents (NNM iSPI Performance for Metrics)" on page 432</p>
<p>CPU monitoring:</p> <ul style="list-style-type: none"> <li>• CPU 5Sec Utilization                     <p>Threshold based on the percentage of a node's CPU usage compared to the total amount of available CPU capacity. This percentage is the average CPU utilization over the prior 5-seconds.</p> </li> <li>• CPU 1Min Utilization                     <p>Threshold based on the percentage of a node's CPU usage compared to the total amount of available CPU capacity. This percentage is the average CPU utilization over the prior 1-minute.</p> </li> <li>• CPU 5Min Utilization                     <p>Threshold based on the percentage of a node's CPU usage compared to the total amount of available CPU capacity. This percentage is the average CPU utilization over the prior 5-minutes.</p> </li> </ul>	<p>See "CPU Incidents (NNM iSPI Performance for Metrics)" on page 433</p>
<p>Disk Space Utilization</p> <p>Threshold based on the percentage of a node's disk space usage compared to the total amount of available disk space.</p>	<p>See "Disk Incidents (NNM iSPI Performance for Metrics)" on page 434</p>
<p>Interface Frame Check Sequence (FCS) monitoring:</p> <ul style="list-style-type: none"> <li>• FCS LAN Error Rate                     <p><i>Local Area Network interfaces only.</i> Threshold based on the</p> </li> </ul>	<p>See "Interface Frame Check Sequence (FCS) Error Rate Incidents (NNM iSPI Performance</p>

**Performance Threshold Incidents (NNM iSPI Performance for Metrics), continued**

Threshold Being Monitored	Incidents
<p>percentage of incoming frames with a bad checksum (CRC value) compared to the total number of incoming frames. Possible causes include collisions at half-duplex, a duplex mismatch, bad hardware (NIC, cable, or port), or a connected device generating frames with bad Frame Check Sequence.</p> <ul style="list-style-type: none"> <li>• FCS WLAN Error Rate</li> </ul> <p><i>Wireless Local Area Network Interfaces only.</i> Threshold based on the percentage of incoming frames with a bad checksum (CRC value) compared to the total number of incoming frames. Possible causes include wireless communication interference, bad hardware (NIC, cable or port), or a connected device generating frames with bad Frame Check Sequence.</p>	<p>for Metrics)" on page 436</p>
<p>Interface Discard Rate monitoring:</p> <ul style="list-style-type: none"> <li>• Input Discard Rate</li> </ul> <p>Threshold based on the percentage of the interface's discarded input packet count compared to the total number of packets received. Packets might be discarded because of a variety of issues, including receive-buffer overflows, congestion, or system specific issues.</p> <ul style="list-style-type: none"> <li>• Output Discard Rate</li> </ul> <p>Threshold based on the percentage of the interface's discarded output packet count compared to the total number of outgoing packets. Packets might be discarded because of a variety of issues, including transmission buffer overflows, congestion, or system specific issues.</p>	<p>See "Interface Input and Output Discard Rate Incidents (NNM iSPI Performance for Metrics)" on page 437.</p>
<p>Interface Error Rate monitoring:</p> <ul style="list-style-type: none"> <li>• Input Error Rate</li> </ul> <p>Threshold based on the percentage of the interface's input packet error count compared to the total number of packets received. What constitutes an error is system specific, but likely includes such issues as bad packet checksums, incorrect header information, and packets that are too small.</p> <ul style="list-style-type: none"> <li>• Output Error Rate</li> </ul> <p>Threshold based on the percentage of the interface's output packet error count compared to the total number of outgoing packets. What constitutes an error is system specific, but likely includes such issues as as collisions and buffer errors.</p>	<p>See "Interface Input and Output Error Rate Incidents (NNM iSPI Performance for Metrics)" on page 439.</p>
<p>Interface Queue monitoring:</p> <ul style="list-style-type: none"> <li>• Input Queue Drops Rate</li> </ul>	<p>See "Input and Output Queue Drop Incidents (NNM iSPI Performance for Metrics)" on page 441.</p>

**Performance Threshold Incidents (NNM iSPI Performance for Metrics), continued**

Threshold Being Monitored	Incidents
<p>Threshold based on the percentage of the interface's dropped input packets compared to the total number of packets received. Possible causes include the input queue being full.</p> <ul style="list-style-type: none"> <li>Output Queue Drops Rate</li> </ul> <p>Threshold based on the percentage of the interface's dropped output packets compared to the total number of outgoing packets. Possible causes include all buffers allocated to the interface being full.</p>	
<p>Interface Utilization monitoring:</p> <ul style="list-style-type: none"> <li>Input Utilization</li> </ul> <p>Threshold based on the percentage of the interface's total incoming octets compared to the maximum number of octets possible (determined by the MIB being used to query <code>ifSpeed</code> of the device and whether the host system supports high-speed counters for interfaces).</p> <div data-bbox="321 898 1062 1283" style="background-color: #f0f0f0; padding: 10px;"> <p><b>Tip:</b> Sometimes the <code>ifSpeed</code> value returned by the device's SNMP agent is not accurate and causes problems with thresholds. If your NNMi role allows, you can override the <code>ifSpeed</code> reported by the SNMP agent:</p> <ol style="list-style-type: none"> <li>Open the problem interface's Interface form.</li> <li>Select the <a href="#">General Tab</a>.</li> <li>Locate the Input/Output Speed section.</li> <li>Change the Input Speed or Output Speed setting.</li> </ol> </div> <ul style="list-style-type: none"> <li>Output Utilization</li> </ul> <p>Threshold based on the percentage of the interface's total outgoing octets compared to the maximum number of octets possible (determined by the MIB being used to query <code>ifSpeed</code> of the device and whether the host system supports high-speed counters for interfaces).</p> <div data-bbox="321 1539 1062 1850" style="background-color: #f0f0f0; padding: 10px;"> <p><b>Tip:</b> Sometimes the <code>ifSpeed</code> value returned by the device's SNMP agent is not accurate and causes problems with thresholds. If your NNMi role allows, you can override the <code>ifSpeed</code> reported by the SNMP agent:</p> <ol style="list-style-type: none"> <li>Open the problem interface's Interface form.</li> <li>Select the <a href="#">General Tab</a>.</li> <li>Locate the Input/Output Speed section.</li> </ol> </div>	<p>See "Interface Input and Output Utilization Incidents (NNM iSPI Performance for Metrics)" on page 443.</p>

**Performance Threshold Incidents (NNM iSPI Performance for Metrics), continued**

Threshold Being Monitored	Incidents
d. Change the Input Speed or Output Speed setting.	
Memory Utilization Threshold based on the percentage of a node's memory usage compared to the total amount of available memory.	See "Memory Incidents (NNM iSPI Performance for Metrics)" on page 446

## Backplane Incidents (*NNM iSPI Performance for Metrics*)

Backplane incidents are available if the HP Network Node Manager iSPI Performance for Metrics Software is installed and your administrator configured performance measurement thresholds. For more information:

Backplane incidents identify backplanes that are over-used or under-used.

You receive backplane incidents when performance is not within the allowable range set by your administrator. Reasons for setting backplane thresholds include:

- Monitor for under-utilization which wastes money
- Monitor for over-utilization, which might result in performance bottlenecks or service provider surcharges (over a pre-specified percentage)

The status of backplane incidents depends on whether the measured value is over or under the allowable range. The following table describes the meaning of Abnormal Range, Low, Nominal, and High.

State Value	Description	Incident	Status
Abnormal Range	The measured value is abnormal based on the computed baseline.	Backplane Abnormal	Warning
Low/None	The measured value is less than the allowable range.	Backplane Out of Range or Malfunctioning	Minor
Nominal	The measured value is within the allowable range. This incident cancels any related High, Low, or None incidents.	No incident is generated	Not applicable
High	The measured value is greater than the allowable range	Backplane Out of Range or Malfunctioning	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 Backplane errors. These appear in the Conclusions lists on the associated Node Component form.

**Possible Conclusions for Backplane Incidents (Node Component Form)**

Conclusion	Status
BackplaneAbnormal	Warning
BackplaneOutOfRangeOrMalfunctioning	Critical

When NNMI determines that the Node Component is within the allowable range, NNMI updates the following attributes:

The Node Component Status is changed to **Normal**.

The Node Component Conclusion is changed to one of the following:

**Conclusions Used to Close Backplane Incidents**

Incident Conclusion	Conclusion to Close the Incident
BackplaneAbnormal	BackplaneNormal
BackplaneOutOfRangeOrMalfunctioning	BackPlaneInRangeAndFunctioning

## Buffer Incidents (*NNM iSPI Performance for Metrics*)

Buffer incidents are available if the HP Network Node Manager iSPI Performance for Metrics Software is installed and your administrator configured performance measurement thresholds. For more information:

Buffer incidents identify nodes that are over-used or under-used.

You receive buffer incidents when performance is not within the allowable range set by your administrator. Reasons for setting buffer thresholds include:

- Monitor for under-utilization which wastes money
- Monitor for over-utilization, which might result in performance bottlenecks or service provider surcharges (over a pre-specified percentage)

The status of buffer incidents depends on whether the measured value is over or under the allowable range. The following table describes the meaning of Abnormal Range, Low, Nominal, and High.



State Value	Description	Incident	Status
Abnormal Range	The measured value is abnormal based on the computed baseline.	Buffer Abnormal	Warning
Low/None	The measured value is less than the allowable range.	Buffer Out of Range or Malfunctioning	Minor
Nominal	The measured value is within the allowable range. This incident cancels any related High, Low, or None incidents.	No incident is generated	Not applicable
High	The measured value is greater than the allowable range	Buffer Out of Range or Malfunctioning	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 Buffer errors. These appear in the Conclusions lists on the associated Node Component form.

#### Possible Conclusions for Buffer Incidents (Node Component Form)

Conclusion	Status
BufferAbnormal	Warning
BufferOutOfRangeOrMalfunctioning	Critical

When NNMi determines that the Node Component is within the allowable range, NNMi updates the following attributes:

The Node Component Status is changed to **Normal**

The Node Component Conclusion is changed to one of the following:

#### Conclusions Used to Close Buffer Incidents

Incident Conclusion	Conclusion to Close the Incident
BufferAbnormal	BufferNormal
BufferOutOfRangeOrMalfunctioning	BufferInRangeAndFunctioning

## CPU Incidents (*NNM iSPI Performance for Metrics*)

CPU incidents are available if the HP Network Node Manager iSPI Performance for Metrics Software is installed and your administrator configured performance measurement thresholds. For more information:

CPU incidents identify nodes that are over-used or under-used.

You receive CPU incidents when performance is not within the allowable range set by your administrator. Reasons for setting CPU thresholds include:

- Monitor for under-utilization which wastes money
- Monitor for over-utilization, which might result in performance bottlenecks or service provider surcharges (over a pre-specified percentage)

Information under the following Incident tabs is updated:

- Correlated Parents
- Correlated Children
- Custom Attributes

The following table describes a combination of conclusions leading to CPU errors. These appear in the Conclusions lists on the associated node form.

**Possible Conclusions for Utilization Incidents (Node form)**

Conclusion	Status
CPUAbnormal	Warning
CPUOutOfRangeOrMalfunctioning	Critical

When NNMi determines that the Node Component is within the allowable range, NNMi updates the following attributes:

The Node Component Status is changed to **Normal**

The Node Component Conclusion is changed to one of the following:

**Conclusions Used to Close CPU Incidents**

Incident Conclusion	Conclusion to Close the Incident
CPUAbnormal	CPUNormal
CPUOutOfRangeOrMalfunctioning	CPUInRangeAndFunctioning

## Disk Incidents (*NNM iSPI Performance for Metrics*)

Disk incidents are available if the HP Network Node Manager iSPI Performance for Metrics Software is installed and your administrator configured performance measurement thresholds. For more information:

Disk incidents identify nodes that are over-used or under-used.

You receive disk incidents when performance is not within the allowable range set by your administrator. Reasons for setting disk thresholds include:

- Monitor for under-utilization which wastes money
- Monitor for over-utilization, which might result in performance bottlenecks or service provider surcharges (over a pre-specified percentage)

The status of disk incidents depends on whether the measured value is over or under the allowable range. The following table describes the meaning of Abnormal Range, Low, Nominal, and High.

State Value	Description	Incident	Status
Abnormal Range	The measured value is abnormal based on the computed baseline.	Disk Abnormal	Warning
Low/None	The measured value is less than the allowable range.	Disk Out of Range or Malfunctioning	Minor
Nominal	The measured value is within the allowable range. This incident cancels any related High, Low, or None incidents.	No incident is generated	Not applicable
High	The measured value is greater than the allowable range	Disk Out of Range or Malfunctioning	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 Disk errors. These appear in the Conclusions lists on the associated Node Component form.

**Possible Conclusions for Disk Incidents (Node Component Form)**

Conclusion	Status
DiskAbnormal	Warning
DiskOutOfRangeOrMalfunctioning	Critical

When NNMi determines that the Node Component is within the allowable range, NNMi updates the following attributes:

The Node Component Status is changed to **Normal**

The Node Component Conclusion is changed to one of the following:

**Conclusions Used to Close Disk Incidents**

Incident Conclusion	Conclusion to Close the Incident
DiskAbnormal	DiskNormal
DiskOutOfRangeOrMalfunctioning	DiskInRangeAndFunctioning

## Interface Frame Check Sequence (FCS) Error Rate Incidents (*NNM iSPI Performance for Metrics*)

Interface Frame Check Sequence (FCS) error rate incidents are available if the HP Network Node Manager iSPI Performance for Metrics Software is installed and your administrator configured performance measurement thresholds. For more information:

FCS error rate incidents identify interfaces that are dropping data.

You receive FCS error rate incidents when error rate threshold is not within the allowable range set by your administrator. Reasons for setting FCS error rate thresholds include:

- Check for corrupted data packets
- Detect configuration mismatches
- Detect faulty hardware

The status of FCS error rate incidents depends on whether the measured value is over or under the allowable range. The following table describes the meaning of Abnormal, Nominal and High.

State Value	Description	Incident	Status
Nominal	The measured value is within the allowable range. This incident cancels any related High, Low, or None incidents.	No incident is generated	Not applicable
High	The measured value is greater than the allowable range	Interface FCS LAN Error Rate High  Interface FCS WLAN Error Rate High	Major

Information under the following Incident tabs is updated:

- Correlated Parents
- Correlated Children
- Custom Attributes

The following table describes a combination of Conclusions leading to FCS LAN errors. These appear in the Conclusions lists on the associated Interface form.

### Possible Conclusions for Interface FCS Error Rate Incidents (Interface form)

Conclusion	Status
InterfaceFCSLANErrorRateHigh	Major
InterfaceFCSWLANErrorRateHigh	Major

When NNMi determines that the FCS LAN Interface Error Rate is within the allowable range, NNMi updates the following attributes:

The Interface Status is changed to **Normal**.

The Interface Conclusion is changed as shown in the following table:

**Conclusions Used to Close FCS Error Rate Incidents**

Incident Conclusion	Conclusion to Close the Incident
InterfaceFCSLANErrorRateHigh	InterfaceFCSLANErrorRateInRange
InterfaceFCSWLANErrorRateHigh	InterfaceFCSLANErrorRateInRange

## Interface Input and Output Discard Rate Incidents (*NNM iSPI Performance for Metrics*)

Interface input and output discard rate incidents are available if the HP Network Node Manager iSPI Performance for Metrics Software is installed and your administrator configured performance measurement thresholds. For more information:

Interface input and output discard rate incidents enable you to identify interfaces that have transmission buffer overflows or are bottlenecks.

You receive interface 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.

State Value	Description	Incident	Status
None	The measured value is zero.	Interface Input Discard Rate None Interface Output Discard Rate None	Normal
Low	The measured value is less than the allowable range.	Interface Input Discard Rate Low Interface Output Discard Rate Low	Normal

State Value	Description	Incident	Status
Nominal	The measured value is within the allowable range. This incident cancels any related High, Low, or None incidents.	No incident is generated	Not applicable
High	The measured value is greater than the allowable range	Interface Input Discard Rate High Interface Output Discard Rate High	Major

Information on the following Incident tabs is updated:

- Correlated Parents
- Correlated Children
- Custom Attributes

The following table describes a combination of conclusions leading to input and output discard rate incidents. These appear in the Conclusions lists on the associated interface and connection or node forms.

**Possible Conclusion Combinations for Input Discard Rate Incidents (Interface, Connection and Node forms)**

Form	Conclusion	Status
Interface	InterfaceInputDiscardRateNone	Normal
Interface	InterfaceInputDiscardRateLow	Normal
Interface	InterfaceInputDiscardRateHigh	Major
Interface	InterfaceOutputDiscardRateNone	Normal
Interface	InterfaceOutputDiscardRateLow	Normal
Interface	InterfaceOutputDiscardRateHigh	Major
Connection	SomeConnectionThresholdValuesHigh	Minor
Connection	AllConnectionThresholdValuesHigh	Critical
Connection	SomeOrAllConnectionThresholdValuesLow	Minor
Connection	SomeOrAllConnectionThresholdValuesNone	Minor
Node	SomeInterfacesOutsideThresholdBoundariesInNode	Minor

When NNMi determines that the Interface Input or Output Discard Rate is within the allowable range, NNMi updates the following attributes:

The Interface Status is changed to **Normal**.

The Interface, Connection, or Node Conclusion is changed as shown in the following table:

**Conclusions Used to Close Interface Input and Output Discard Rate Incidents**

Incident Conclusion	Conclusion to Close the Incident
InterfaceInputDiscardRateNone	InterfaceInputDiscardRateNominal
InterfaceInputDiscardRateLow	InterfaceInputDiscardRateNominal
InterfaceInputDiscardRateHigh	InterfaceInputDiscardRateNominal
InterfaceOutputDiscardRateNone	InterfaceOutputDiscardRateNominal
InterfaceOutputDiscardRateLow	InterfaceOutputDiscardRateNominal
InterfaceOutputDiscardRateHigh	InterfaceOutputDiscardRateNominal
SomeConnectionThresholdValuesHigh	ConnectionWithinThresholdBoundaries
AllConnectionThresholdValuesHigh	ConnectionWithinThresholdBoundaries
SomeOrAllConnectionThresholdValuesLow	ConnectionWithinThresholdBoundaries
SomeOrAllConnectionThresholdValuesNone	ConnectionWithinThresholdBoundaries
SomeInterfacesOutsideThresholdBoundariesInNode	AllInterfacesWithinThresholdBoundariesInNode

## Interface Input and Output Error Rate Incidents (*NNM iSPI Performance for Metrics*)

Interface input and output error rate incidents are available if the HP Network Node Manager iSPI Performance for Metrics Software is installed and your administrator configured performance measurement thresholds. For more information:

Interface input and output error rate incidents identify interfaces that are dropping data.

You receive interface 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.

State Value	Description	Incident	Status
None	The measured value is zero.	Interface Input Error Rate None	Normal

State Value	Description	Incident	Status
		Interface Output Error Rate None	
Low	The measured value is less than the allowable range.	Interface Input Error Rate Low Interface Output Error Rate Low	Normal
Nominal	The measured value is within the allowable range. This incident cancels any related High, Low, or None incidents.	No incident is generated	Not applicable
High	The measured value is greater than the allowable range	Interface Input Error Rate High Interface Output Error Rate High	Major

Information on the following Incident tabs is updated:

- Correlated Parents
- Correlated Children
- Custom Attributes

The following table describes a combination of conclusions leading to interface input error rate incidents. These appear in the Conclusions lists on the associated interface and connection or node forms.

**Possible Conclusion Combinations for Input Error Rate Incidents (Interface, Connection and Node forms)**

Form	Conclusion	Status
Interface	InterfaceInputErrorRateNone	Normal
Interface	InterfaceInputErrorRateLow	Normal
Interface	InterfaceInputErrorRateHigh	Major
Interface	InterfaceOutputErrorRateNone	Normal
Interface	InterfaceOutputErrorRateLow	Normal
Interface	InterfaceOutputErrorRateHigh	Major
Connection	SomeConnectionThresholdValuesHigh	Minor



**Possible Conclusion Combinations for Input Error Rate Incidents (Interface, Connection and Node forms), continued**

Form	Conclusion	Status
Connection	AllConnectionThresholdVauesHigh	Critical
Node	SomeInterfacesOutsideThresholdBoundariesInNode	Minor

When NNMi determines that the Interface Input or Output Error Rate is within the allowable range, NNMi updates the following attributes:

The Interface Status is changed to **Normal**.

The Interface Conclusion is changed to one of the following:

**Conclusions Used to Close Interface Input and Output Error Rate Incidents**

Incident Conclusion	Conclusion to Close the Incident
InterfaceInputErrorRateNone	InterfaceInputErrorRateNominal
InterfaceInputErrorRateLow	InterfaceInputErrorRateNominal
InterfaceInputErrorRateHigh	InterfaceInputErrorRateNominal
InterfaceOutputErrorRateNone	InterfaceOutputErrorRateNominal
InterfaceOutputErrorRateLow	InterfaceOutputErrorRateNominal
InterfaceOutputErrorRateHigh	InterfaceOutputErrorRateNominal
SomeConnectionThresholdValuesHigh	ConnectionWithinThresholdBoundaries
AllConnectionThresholdValuesHigh	ConnectionsWithinThresholdBoundaries
SomeInterfacesOutsideThresholdBoundariesInNode	AllInterfacesWithinThresholdBoundariesInNode

## Input and Output Queue Drop Incidents (*NNM iSPI Performance for Metrics*)

Input Queue Drop and Output Queue Drop incidents are available if the HP Network Node Manager iSPI Performance for Metrics Software is installed and your administrator configured performance measurement thresholds. For more information:

Interface input and output queue drop incidents enable you to identify interfaces that have transmission buffer overflows or are bottlenecks.

You receive input and output queue drop incidents when a discard rate is not within the allowable range set by your administrator. For example, the queue drop rate must not exceed 10 percent. Reasons for setting queue drop rate thresholds include:

- Check for large data packets
- Monitor bottlenecks

- Detect faulty hardware

The status of input and output queue drop incidents depends on whether the measured value is over the allowable range. The following table describes the meaning of Nominal and High.

State Value	Description	Incident	Status
Nominal	The measured value is within the allowable range. This incident cancels any related High, Low, or None incidents.	No incident is generated	Not applicable
High	The measured value is greater than the allowable range	Interface Input Queue Drops High  Interface Output Queue Drops High	Major

Information on the following Incident tabs is updated:

- Correlated Parents
- Correlated Children
- Custom Attributes

The following table describes a combination of conclusions leading to input and output queue drop rate incidents. These appear in the Conclusions lists on the associated interface form.

**Possible Conclusions for Input Queue Drop Incidents (Interface, Connection and Node forms)**

Form	Conclusion	Status
Interface	InterfaceInputQueueDropsHigh	Major
Interface	InterfaceOutputQueueDropsHigh	Major
Connection	SomeConnectionThresholdValuesHigh	Minor
Connection	AllConnectionThresholdValuesHigh	Critical
Node	SomeInterfacesOutsideThresholdBoundariesInNode	Minor

When NNMi determines that the Queue Drops are within the allowable range, NNMi updates the following attributes:

The Interface Status is changed to **Normal**.

The Interface, Connection, or Node Conclusion is changed as shown in the following table:

### Conclusions Used to Close Input and Output Queue Drops Incidents

Incident Conclusion	Conclusion to Close the Incident
InterfaceInputQueueDropsHigh	InterfaceInputQueueDropsRateInRange
InterfaceOutputQueueDropsHigh	InterfaceOutputQueueDropsRateInRange
SomeConnectionThresholdValuesHigh	ConnectionWithinThresholdBoundaries
AllConnectionThresholdValuesHigh	ConnectionWithinThresholdBoundaries
SomeInterfacesOutsideThresholdBoundariesInNode	AllInterfacesWithinThresholdBoundariesInNode

## Interface Input and Output Utilization Incidents (*NNM iSPI Performance for Metrics*)

Input and output utilization incidents are available if the HP Network Node Manager iSPI Performance for Metrics Software is installed and your administrator configured performance measurement thresholds. For more information:

Input and output utilization incidents identify interfaces that are over-used or under-used.

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 might result in performance bottlenecks or service provider surcharges (over a pre-specified percentage)

The status of input and output utilization incidents depends on whether the measured value is over or under the allowable range. The following table describes the meaning of Abnormal Range, None, Low, Nominal, and High.

State Value	Description	Incident	Status
Abnormal Range	The measured value is abnormal based on the computed baseline.	Interface Input Utilization Abnormal Interface Output Utilization Abnormal	Warning
None	The measured value is zero.	Interface Input Utilization None Interface Output Utilization None	Minor
Low	The measured value is less than the allowable range.	Interface Input Utilization Low	Major

State Value	Description	Incident	Status
Nominal	The measured value is within the allowable range. This incident cancels any related High, Low, or None incidents.	No incident is generated	Not applicable
High	The measured value is greater than the allowable range	Interface Output Utilization High	Major

Information under the following Incident tabs is updated:

- Correlated Parents
- Correlated Children
- Custom Attributes

The following tables describes a combination of conclusions leading to input and output utilization errors. These appear in the Conclusions lists on the associated Interface and Connection or Node forms.

**Possible Conclusion Combinations for Input Utilization Incidents (Interface, Connection, and Node)**

Form	Conclusion	Status
Interface	InterfaceInputUtilizationAbnormal	Warning
Interface	InterfaceInputUtilizationNone	Minor
Interface	InterfaceInputUtilizationLow	Major
Interface	InterfaceOutputUtilizationAbnormal	Warning
Interface	InterfaceOutputUtilizationNone	Minor
Interface	InterfaceOutputUtilizationHigh	Major
Connection	SomeConnectionThresholdValuesHigh	Minor
Connection	AllConnectionThresholdValuesHigh	Critical
Connection	SomeOrAllConnectionThresholdValuesLow	Minor
Node	SomeInterfacesOutsideThresholdBoundariesInNode	Minor

When NNMi determines that the Interface Input or Output Utilization Rate is within the allowable range, NNMi updates the following attributes:

The Interface Status is changed to **Normal**.

The Interface Conclusion is changed to one of the following:

### Conclusions Used to Close Interface Input and Output Utilization Incidents

Incident Conclusion	Conclusion to Close the Incident
InterfaceInputUtilizationAbnormal	InterfaceInputUtilizationNominal
InterfaceInputUtilizationNone	InterfaceInputUtilizationNominal
InterfaceInputUtilizationLow	InterfaceInputUtilizationNominal
InterfaceOutputUtilizationAbnormal	InterfaceOutputUtilizationNormal
InterfaceOutputUtilizationNone	InterfaceOutputUtilizationNominal
InterfaceOutputUtilizationHigh	InterfaceOutputUtilizationNominal
SomeConnectionThresholdValuesHigh	ConnectionWithinThresholdBoundaries
AllConnectionThresholdValuesHigh	ConnectionWithinThresholdBoundaries
SomeOrAllConnectionThresholdValuesLow	ConnectionWithinThresholdBoundaries
SomeInterfacesOutsideThresholdBoundariesInNode	AllInterfacesWithinThresholdBoundariesInNode

## Management Address ICMP Response Time Incidents

Management address Internet Control Message Protocol (ICMP) response time incidents enable you to identify high or abnormal ICMP response time from the NNMi management server to the selected node.

You receive response time incidents when the ICMP response time for the selected management address is not within the allowable range set by your administrator. Reasons for setting ICMP response time rate thresholds include identifying changes in network performance from the management server to the selected node.

The State value returned for the node depends on whether the measured value is over the allowable range or outside of the configured baseline settings. The following table describes the meaning of **High** and **Abnormal**.

State Value	Description	Incident	Status
Abnormal	The measured value is abnormal based on the computed baseline.	Management Address ICMP Response Time Abnormal	Warning
High	The measured value is greater than the allowable range.	Management Address ICMP Response Time High	Warning

Information on the following Incident tabs is updated:

- Correlated Parents
- Correlated Children

- Custom Attributes

The following table describes a combination of conclusions leading to Management Address ICMP response time incidents. These appear in the Conclusions lists on the associated interface form.

**Possible Conclusions for Management Address ICMP Response Time Incidents (SNMP Agent form)**

Conclusion	Status
ManagementAddressICMPResponseTimeAbnormal	Warning
ManagementAddressICMPResponseTimeHigh	Warning

When NNMi determines that the Management Address ICMP Response Time is within the allowable range, NNMi updates the following attributes:

The SNMP Agent Status is changed to **Normal**.

The SNMP Agent Conclusion is changed to one of the following:

**Conclusions Used to Close Management Address ICMP Response Time Incidents**

Incident Conclusion	Conclusion to Close the Incident
ManagementAddressICMPResponseTimeAbnormal	ManagementAddressICMPResponseTimeNormal
ManagementAddressICMPResponseTimeHigh	ManagementAddressICMPResponseTimeNominal

## Memory Incidents (*NNM iSPI Performance for Metrics*)

Memory incidents are available if the HP Network Node Manager iSPI Performance for Metrics Software is installed and your administrator configured performance measurement thresholds. For more information:

Memory incidents identify nodes that are over-used or under-used.

You receive memory incidents when performance is not within the allowable range set by your administrator.

The status of memory incidents depends on whether the measured value is over or under the allowable range. The following table describes the meaning of Abnormal Range, Low, Nominal, and High.

State Value	Description	Incident	Status
Abnormal Range	The measured value is abnormal based on the computed baseline.	Memory Abnormal	Warning
Nominal	The measured value is within the allowable range.	No incident is	Not

State Value	Description	Incident	Status
	This incident cancels any related High, Low, or None incidents.	generated	applicable
High	The measured value is greater than the allowable range	Memory Out of Range Or Malfunctioning	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 Memory incidents. These appear in the Conclusions lists on the associated Node Component form.

**Possible Conclusions for Memory Incidents (Node Component form)**

Conclusion	Status
MemoryAbnormal	Warning
MemoryOutOfRangeOrMalfunctioning	Critical

When NNMi determines that the Node Component is within the allowable range, NNMi updates the following attributes:

The Node Component Status is changed to **Normal**.

The Node Component Conclusion is changed to one of the following:

**Conclusions Used to Close Memory Incidents**

Incident Conclusion	Conclusion to Close the Incident
MemoryAbnormal	MemoryDiskNormal
MemoryOutOfRangeOrMalfunctioning	MemoryInRangeAndFunctioning

## Find a Node

As part of the investigation and diagnosis process, you might want to search the NNMi database for details about 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.

See "[Access Node Details](#)" on page 287 and [Access More Details \(Forms and Analysis Pane\)](#) for a description of additional ways to access node details.

**To find information about a node:**

1. From the console, select **Tools** → **Find Node**.
2. In the **Find Node** dialog, enter one of the following *case-sensitive* known values for the node of interest:

**"Find Node" Options**

Possible Values	Description
Hostname	<p>The current value of the <i>fully-qualified, case-sensitive</i> Hostname attribute as it appears on the Node form.</p> <p>NNMi follows a set of rules to dynamically generate the value stored in the NNMi database for each Node's Hostname. Click here for details.</p> <ul style="list-style-type: none"> <li>■ If the Node supports SNMP, NNMi requests the Hostname using the IP Address of the associated SNMP agent (the Management Address attribute value on the Node form).                     <p>When the NNMi administrator chooses <b>Enable SNMP Address Rediscovery</b> <input checked="" type="checkbox"/> in the Communication Configuration:</p> <ul style="list-style-type: none"> <li>○ If the SNMP Agent does not respond, NNMi checks for another Management Address to request the Hostname, and the Hostname could change.</li> <li>○ If the SNMP Agent associated with the node changes, the Management Address and Hostname could change.</li> </ul> <p>When the NNMi administrator disables <b>Enable SNMP Address Rediscovery</b> <input type="checkbox"/> in the Communication Configuration:</p> <ul style="list-style-type: none"> <li>○ If the SNMP Agent does not respond, NNMi uses the previously gathered Management Address attribute value to request the Hostname.</li> <li>○ If the SNMP Agent associated with the node changes, NNMi uses the previously gathered Management Address attribute value to request the Hostname.</li> </ul> </li> <li>■ If the Node does not support SNMP, no Management Address is available. NNMi requests a Hostname starting with the lowest IP Address associated with the node (a Discovery Seed value or an IP address value gathered from a neighboring device). NNMi uses the first Hostname provided. The Hostname might change during a future discovery cycle.</li> </ul> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p><b>Note:</b> NNMi administrators can use NNMi property file settings to change the way NNMi determines Hostname values:</p> <ul style="list-style-type: none"> <li>■ <code>nms-topology.properties</code> file settings:                             <p>If DNS is the source of the Node's Hostname, there are three choices. By default NNMi uses the exact Hostname from your network configuration. It is possible to change NNMi behavior to convert Hostnames to all uppercase or all lowercase. See the "Modifying NNMi</p> </li> </ul> </div>



### "Find Node" Options, continued

Possible Values	Description
	<p>Normalization Properties" section of the <i>HP Network Node Manager i Software Deployment Reference</i>, which is available at:  <a href="http://h20230.www2.hp.com/selfsolve/manuals">http://h20230.www2.hp.com/selfsolve/manuals</a>.</p> <ul style="list-style-type: none"> <li> <b>nms-disco.properties</b> file settings:                      The Hostname is either requested from the Node's lowest loopback interface IP address that resolves to a Hostname or requested from the Node's designated Management Address (SNMP agent address). With either choice, when no IP address resolves to a Hostname, the IP address itself becomes the Hostname. See the "Maintaining NNMi" chapter of the <i>HP Network Node Manager i Software Deployment Reference</i>, which is available at:  <a href="http://h20230.www2.hp.com/selfsolve/manuals">http://h20230.www2.hp.com/selfsolve/manuals</a>.                 </li> </ul>
IP address of any interface	The IP address of any interface in the node.
System Name	The current value of the MIB-II <code>sysName</code> that is obtained from the node's SNMP agent (case-sensitive) as it appears in the System Name attribute on Node form. For example <code>cisco5500.abc.example.com</code>
Name	<p>The current value of the Name attribute as it appears on the Node form.</p> <p>The NNMi administrator configures how NNMi populates this attribute through two configuration settings: (1) The <b>Node Name Resolution</b> attributes in Discovery Configuration (full or short DNS name, full or short sysName, IP address). (2) The Name <i>might be</i> converted to all uppercase or all lowercase (depending on how the NNMi administrator configured settings in the <code>nms-topology.properties</code> file). See the "Modifying NNMi Normalization Properties" section of the <i>HP Network Node Manager i Software Deployment Reference</i>, which is available at:  <a href="http://h20230.www2.hp.com/selfsolve/manuals">http://h20230.www2.hp.com/selfsolve/manuals</a>.</p>

3. Click **Find**.

NNMi searches the database to find a matching value in any of the attributes listed in the preceding table.

NNMi displays the [Node form](#) of the *first* match. If no match is found, NNMi displays an error message.

## Find the Attached Switch Port

**Tools** → **Find Attached Switch Port** helps you investigate and diagnose problems when you need to quickly determine which switch a problem End Node uses. For example, if an End Node in

your network has a potential virus, you can identify the switch through which that End Node connects to your network. Then, you can prevent the virus from moving to other nodes in your network.

(*NNMi Advanced - Global Network Management feature*) The Global Manager and the Regional Manager maintain separate sets of data. Conclusions about each Node are derived from the available data and can sometimes be different. Regional Managers forward the results of each Spiral Discovery cycle to the Global Manager. The Regional Manager can have a Node Group filter configured to limit the amount of data that is forwarded to the Global Manager. Filters are usually unnecessary for Global Network Management. Do not filter out nodes that are important for connectivity in your network environment to ensure NNMi has the data needed for accurate root cause analysis.

- The Global Manager might know information about why a connection from one site to another is down, but the Regional Manager just knows that the router connected to that remote site has an interface that is down. Use **Actions** → **Regional Manager Console** to see the other perspective.
- When troubleshooting a Node on the Global Manager, you can use **Actions** → **Open from Regional Manager** to see the latest Node information on the Regional Manager.

**Tip:** You can also use the `nnmfindattachedswport.ovpl` command to find which Switch an End Node uses to reach your network.

**To find which  Switch an End Node uses to reach your network:**

1. From the console, select **Tools** → **Find Attached Switch Port**.
2. Navigate to the **End Node** field, and enter one of the following *case-sensitive* known values for the end Node.

**"Find Attached Switch Port" Options**

Possible Values	Description
Hostname	<p>The End Node's <i>fully-qualified, case-sensitive</i> Hostname value.</p> <p>The End Node can be either of the following:</p> <ul style="list-style-type: none"> <li>■ A device in your network environment that has not been discovered by NNMi (no corresponding Node object in the NNMi database).</li> <li>■ A Node previously discovered by NNMi. The Hostname you provide must match the current <i>case-sensitive</i> value of the end Node's <i>Hostname</i> attribute on the "Node Form" on page 50. See "Access Node Details" on page 287 and <a href="#">Access More Details (Forms and Analysis Pane)</a> for methods of looking up the current Hostname value.</li> </ul> <p>NNMi follows a set of rules to dynamically generate the value stored in the NNMi database for each Node's Hostname. <a href="#">Click here for details.</a></p> <ul style="list-style-type: none"> <li>○ If the Node supports SNMP, NNMi requests the Hostname using the IP Address of the associated SNMP agent (the Management Address attribute value on the Node form).</li> </ul>

## "Find Attached Switch Port" Options, continued

Possible Values	Description
	<p>When the NNMi administrator chooses <b>Enable SNMP Address Rediscovery</b> <input checked="" type="checkbox"/> in the Communication Configuration:</p> <ul style="list-style-type: none"><li>○ If the SNMP Agent does not respond, NNMi checks for another Management Address to request the Hostname, and the Hostname could change.</li><li>○ If the SNMP Agent associated with the node changes, the Management Address and Hostname could change.</li></ul> <p>When the NNMi administrator disables <b>Enable SNMP Address Rediscovery</b> <input type="checkbox"/> in the Communication Configuration:</p> <ul style="list-style-type: none"><li>○ If the SNMP Agent does not respond, NNMi uses the previously gathered Management Address attribute value to request the Hostname.</li><li>○ If the SNMP Agent associated with the node changes, NNMi uses the previously gathered Management Address attribute value to request the Hostname.</li><li>○ If the Node does not support SNMP, no Management Address is available. NNMi requests a Hostname starting with the lowest IP Address associated with the node (a Discovery Seed value or an IP address value gathered from a neighboring device). NNMi uses the first Hostname provided. The Hostname might change during a future discovery cycle.</li></ul> <p><b>Note:</b> NNMi administrators can use NNMi property file settings to change the way NNMi determines Hostname values:</p> <ul style="list-style-type: none"><li>○ <code>nms-topology.properties</code> file settings: If DNS is the source of the Node's Hostname, there are three choices. By default NNMi uses the exact Hostname from your network configuration. It is possible to change NNMi behavior to convert Hostnames to all uppercase or all lowercase. See the "Modifying NNMi Normalization Properties" section of the <i>HP Network Node Manager i Software Deployment Reference</i>, which is available at: <a href="http://h20230.www2.hp.com/selfsolve/manuals">http://h20230.www2.hp.com/selfsolve/manuals</a>.</li><li>○ <code>nms-disco.properties</code> file settings: The Hostname is either requested from the Node's lowest loopback interface IP address that resolves to a Hostname or requested from the Node's designated Management Address (SNMP agent address). With either choice, when no IP address resolves to a Hostname, the IP address itself becomes the Hostname. See the</li></ul>

### "Find Attached Switch Port" Options, continued

Possible Values	Description
	"Maintaining NNMi" chapter of the <i>HP Network Node Manager i Software Deployment Reference</i> , which is available at: <a href="http://h20230.www2.hp.com/selfsolve/manuals">http://h20230.www2.hp.com/selfsolve/manuals</a> .
IP address of any interface	The current value of any IP address associated with the End Node. <i>NNMi Advanced</i> . Either IPv4 or IPv6 allowed.
MAC address	The current value of the MAC (Media Access Control) address of any interface in the End Node.

3. Click **Find**. NNMi searches *existing data in the NNMi database* for a match, searching through all known Layer 2 information previously gathered from switch forwarding tables in your network environment. NNMi does not generate SNMP traffic to gather additional data for this search.

NNMi displays a report about the  Switch attached to the specified End Node:

- Hostname of the Switch (click the Hostname link to open the switch's Node form).
- Interface Name value (click the Interface link to open the switch's relevant Interface form).
- VLAN Id and Global VLAN Name, if any.

## 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, 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.

(*NNMi Advanced - Global Network Management feature*) The Global Manager and the Regional Manager maintain separate sets of data. Conclusions about each Node are derived from the available data and can sometimes be different. Regional Managers forward the results of each Spiral Discovery cycle to the Global Manager. The Regional Manager can have a Node Group filter configured to limit the amount of data that is forwarded to the Global Manager. Filters are usually unnecessary for Global Network Management. Do not filter out nodes that are important for connectivity in your network environment to ensure NNMi has the data needed for accurate root cause analysis.

- The Global Manager might know information about why a connection from one site to another is down, but the Regional Manager just knows that the router connected to that remote site has an interface that is down. Use **Actions** → **Regional Manager Console** to see the other perspective.
- When troubleshooting a Node on the Global Manager, you can use **Actions** → **Open from Regional Manager** to see the latest Node information on the Regional Manager.

**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 that has 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 that has attached end nodes you want to display; for example **Nodes**.
- iii. From the table view, select 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, select the row that represents the switch of interest.
- iii. Select **Actions** → **Maps** → **Layer 2 Neighbor View**, **Layer 3 Neighbor View**, **Node Group Map**, or **Path View**.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

- iv. In the map, click the map symbol representing the switch of interest.

- **Navigate to a form:**

- i. From a table view, double-click 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:

- The Name of the Interface to which the Node is attached
- The identification number of the VLAN (VLAN ID) to which the Node belongs
- The name of the VLAN to which the Node belongs
- DNS-resolvable hostname
- MAC address of the connected interface
- IP address

Note the following:

- If the end node does not have a DNS-resolvable hostname, NNMi uses the node's IP address for both the Hostname value and the IP Address value.
- If NNMi is unable to locate any information about end nodes attached to the selected switch, NNMi displays a message that no end nodes were found.

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 449

## 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. NNMi displays the ping results, including reply times and ping statistics.

### From an incident view:

1. Select the row representing an incident that has a source node you want to ping.
2. Select **Actions** → **Node Access** → **Ping (from server)**.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

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 in which the interface resides, not the interface itself.

(*NNMi Advanced*) If the Global Network Management feature is enabled and you are signed into a Global Manager:

- Node managed by the Global Manager = **Actions** → **Ping** issues an ICMP request from the Global Manager (NNMi management server).
- Node managed by a Regional Manager = **Actions** → **Ping** accesses that Regional Manager (NNMi management server) and issues the ICMP request.

**Note:** You must sign into that Regional Manager unless your network environment enables Single Sign-On (SSO) to that Regional Manager through the Global Manager. For more information, see the "Configuring Single Sign-On for Global Network Management" section in the *HP Network Node Manager i Software Deployment Reference*, which is available at:  
<http://h20230.www2.hp.com/selfsolve/manuals>.

### 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, select 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, select the row that represents the node or IP address.
- c. Select **Actions** → **Maps** → **Layer 2 Neighbor View**, **Layer 3 Neighbor View** 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, double-click 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 → Node Access → Ping (from server)**

(*NNMi Advanced*) If the Global Network Management feature is enabled and you are signed into a Global Manager:

- Node managed by the Global Manager = Actions → Ping issues an ICMP request from the Global Manager (NNMi management server).
- Node managed by a Regional Manager = Actions → Ping accesses that Regional Manager (NNMi management server) and issues the ICMP request.

**Note:** You must sign into that Regional Manager unless your network environment enables Single Sign-On (SSO) to that Regional Manager through the Global Manager. For more information, see the “Configuring Single Sign-On for Global Network Management” section in the *HP Network Node Manager i Software Deployment Reference*, which is available at:  
<http://h20230.www2.hp.com/selfsolve/manuals>.

## 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 the following:

- 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 265 for more information.
- The starting node is the NNMi management server on which you are running the traceroute command.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

**To access the traceroute command:**

1. Do one of the following:

**Navigate to an Incidents view and select the incident that has the source node's route you want to trace:**

- a. From the workspace navigation panel, select the workspace of interest; for example, **Incident Management**.
- b. Click the view that contains the incident that has the source node's route you want to trace; for example **My Open Incidents**.
- c. From the table view, select the row representing the incident that has a source node's route you want to trace.


**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 that has the route you want to trace; for example **Nodes**.
- c. From the table view, select the row representing the node that has the route you want to trace.

**Navigate to a map view and select a node:**

- a. From the workspace navigation panel, select the workspace of interest; for example, **Topology Maps**.
- b. Click the view that contains the node that has the route you want to trace; for example **Initial Discovery Progress** or **Network Overview**.
- c. From the map view, click the node that has the route you want to trace.

**Navigate to a Node form:**

- From a table view, double-click the row representing the object that has the route you want to trace.
  - From a map view, click the node of interest on the map and click the  Open icon.
2. Select **Actions** → **Node Access** → **Trace Route (from server)**.

NNMi displays the output from traceroute, including the lists of routers that are traversed to reach the destination node.

## Establish Contact with a Node (Telnet or Secure Shell)

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 or Secure Shell (ssh) command from the NNMi console Actions menu.

**Note:** If you cannot access Telnet or ssh from your Web browser, your operating system or Web browser might not enable Telnet or Secure Shell by default. If you are an NNMi



administrator, see the "Configuring the Telnet and SSH Protocols for Use by NNMi" chapter of the *HP Network Node Manager i Software Deployment Reference* for more information.

**To establish contact with a node using Telnet:**

1. Do one of the following:

**Navigate to an incident view:**

- a. Select the row representing the incident that has the source node you want to access using Telnet.
- b. Select **Actions** → **Node Access** → **Telnet (from client)**.

**Note:** NNMi uses Telnet to access the source node of the incident. It does not use Telnet on the source object. For example, if the incident is related to an interface, NNMi uses Telnet to access the node in which the interface resides, not to the interface itself.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.


**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 you want to access using Telnet; for example **Nodes**.
- c. From the table view, select the row representing the node you want to access using Telnet.

**Navigate to a map view and select a node:**

- a. From the workspace navigation panel, select the workspace of interest; for example, **Topology Maps**.
- b. Click the view that contains the node you want to access using Telnet; for example **Initial Discovery Progress** or **Network Overview**.
- c. From the map view, click the node you want to access using Telnet.

**To navigate to a Node form:**

- From a table view, double-click the row representing the node of interest.
- From a map view, click the node of interest on the map and click the  Open icon.

2. Select **Actions** → **Node Access** → **Telnet (from client)**.

**To establish contact with a node using Secure Shell:**

1. Do one of the following:

**Navigate to an incident view:**

- a. Select the row representing the incident that has the source node you want to access using Secure Shell.
- b. Select **Actions** → **Node Access** → **Secure Shell (from client)**.

**Note:** NNMi uses Secure Shell to access the source node of the incident. It does not use Secure Shell on the source object. For example, if the incident is related to an interface, NNMi uses Secure Shell to access the node in which the interface resides, not to the interface itself.


**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 you want to access using Secure Shell; for example **Nodes**.
- c. From the table view, select the row representing the node you want to access using Secure Shell.

**Navigate to a map view and select a node:**

- a. From the workspace navigation panel, select the workspace of interest; for example, **Topology Maps**.
- b. Click the view that contains the node you want to access using Secure Shell; for example **Initial Discovery Progress** or **Network Overview**.
- c. From the map view, click the node you want to access using Secure Shell.

**To navigate to a Node form:**

- From a table view, double-click the row representing the node of interest.
  - From a map view, click the node of interest on the map and click the  Open icon.
2. Select **Actions** → **Node Access** → **Secure Shell (from client)**.


NNMi displays a browser window and a Secure Shell window.

## Check Status Details for a Node Group

NNMi can generate a Status Details report about the a particular Node Group showing how many nodes are currently within each possible *status* (see [Status Color and Meaning for Objects](#)). The Status Details window automatically refreshes Status Detail information every 5 minutes:

- Using a table view, check the status details for a Node Group.
  - a. Navigate to the Node Groups view of interest (see "[Node Groups View \(Inventory\)](#)" on page 44 or "[Node Groups View \(Monitoring\)](#)" on page 282).
  - b. Select the row representing the Node Group of interest.
  - c. Select **Actions** → **Status Details**.

**Tip:** You can right-click any object in a table or map view to access the **Actions** menu.

- d. 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
- Using a map view, to check the status details for a Node Group.
  - a. From the workspace navigation panel, select the **Topology** workspace.
  - b. Select **Node Group Overview**.
  - c. Select the  Node Group symbol of interest.
  - d. Select **Actions** → **Status Details**.
  - e. 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

When diagnosing and troubleshooting problems, you might want to check the status for only a particular set of nodes. Your network administrator can group sets of nodes into Node Groups. For example, all important Cisco routers or all routers in a particular building. See [About Node and Interface Groups](#) for more information about how your NNMi administrator sets up Node Groups. See "[Filter Views by Node or Interface Group](#)" on page 26 for more information about filtering views using Node Groups.

# Chapter 10

---

## 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** → **NNMi 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.

### To check the health of the State Poller and Custom Poller:

1. From the NNMi console, select **Help** → **System Information**. For more information, see [Displaying NNMi System Information](#).

2. Navigate to the **State Poller** tab.

NNMi displays the status of the State Poller, including details about collections, queues, and currently managed objects.

3. Navigate to the **Custom Poller** tab.

NNMi displays the status of the Custom Poller, including details about collections, queues, and currently managed objects.

---

# Glossary

## A

---

### AES

Advanced Encryption Standard

### Anycast Rendezvous Point IP Address

Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

## B

---

### BGP

Border Gateway Protocol

## C

---

### Causal Engine

The NNMi Causal Engine analyzes the health of your network and provides the ongoing health status reading for each device. The Causal Engine also extensively evaluates problems and determines the root cause for you, whenever possible, sending incidents to notify you of problems. Any incident generated from a Causal Engine management event has an Origin of NNMi in your incident views.

### CBC

Cipher Block Chaining

### CE

Customer Edge router. The router in your network that sends data to an Internet Service Provider's router (the Provider Edge) on the path to the data's final destination.

### Custom Node Collection

A Custom Node Collection identifies a topology node that has at least one associated Custom Poller Policy. Because a topology node can be associated with more than one Policy, the same topology node might appear in multiple Custom Node Collections.

### Custom Polled Instance

A Custom Polled Instance represents the results of a MIB expression when it is evaluated against a node. The first time a MIB Expression is validated with discovery information, the results appear in the Monitoring workspace's Custom Polled Instances view. The Custom Polled Instance is updated whenever a change in State occurs and includes the most recent polled value that caused the State to change. These results are then used to determine the Status of the associated Custom Node Collection.

### Custom User Groups

Custom User Groups are the User Groups that you create. These User Groups are additional to the NNMi User Groups, which are those User Groups that NNMi provides.

## D

---

### DES

Data Encryption Standard

## E

---

### EIGRP

Enhanced Interior Gateway Routing Protocol

## **EVPN**

Ethernet Virtual Private Network.

## **G**

---

### **global unicast address**

(2000:: to 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff) A publically routable IPv6 unicast address, used for communication between nodes anywhere on the internet. The first part of the address is a global routing prefix in the 2000::/3 address space for your organization (assigned by the Internet Service Providers). The complete host address can either be manually configured or automatically assigned using IPv6 auto-configuration and neighbor discovery.

## **H**

---

### **HMAC**

Hash-based Message Authentication Code

### **hops**

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.

### **HSRP**

Hot Standby Router Protocol

## **I**

---

### **IPv6 link-local address**

A non-routable IPv6 unicast address only used for communication with other nodes on the same link (LAN or VLAN). Link local addresses cannot be used for communication that must be forwarded through a router. IPv6 auto-configuration automatically assigns a unique link local address in the fe80::/10 address space to each IPv6-enabled interface on a system.

## **ISIS**

Intermediate System to Intermediate System Protocol

## **K**

---

### **Key Incident**

Incidents with both: (1) Severity = other than Normal. (2) Correlation Nature = equal to Root Cause, Service Impact, Stream Correlation, Rate Stream Correlation, Info, or None.

## **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 switch-routers 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**

Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two

Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface). When you double-click the thick line, it converts into multiple thin lines representing the participating Aggregation Member Layer 2 Connections with their Aggregation Member Interfaces at each end of the lines.

**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 Number 24, softwareloopback from the IANA ifType-MIB.

---

**M****MAC address**

The Media Access Control address (hardware address or physical address) that the factory burns into a network adapter or device with built-in networking capability. A MAC address has six pairs of hexadecimal digits, separated by colons or dashes. For example 02:1F:33:16:BC:55

**MAC addresses**

The Media Access Control address (hardware address or physical address) that the factory burns into a network adapter or device with built-in networking

capability. A MAC address has six pairs of hexadecimal digits, separated by colons or dashes. For example 02:1F:33:16:BC:55

**MD5**

Message-Digest algorithm 5

**MPLS**

Multiprotocol Label Switching

**multicast address**

Used to identify a group of hosts joined into a group. IPv4 multicast addresses are in the range 224.0.0.0 to 239.255.255.255 and IPv6 multicast addresses have the prefix ff00::/8.

**multiconnection**

A multiconnection is a thick line on a map view between two Node icons, two Node Group icons, or between a Node icon and a Node Group icon (with no Interface icon or IP Address icon at either end of the line). This thick line represents a set of multiple connections that have been combined to preserve space and simplify the map. Your NNMi administrator specifies the number of connections that must exist before NNMi condenses them into a multiconnection line (User Interface Configuration's Multiconnection Threshold attribute). Double-click the thick line to convert it into the original set of connections with Interface icons or IP Address icons at either end of the lines.

---

**N****NAT**

Network Address Translation. NNMi supports the following protocols: Static Network Address Translation, Dynamic Network Address Translation, Dynamic Port Address Translation.

## NNMi Role

Determined by your membership in one of four special NNMi User Groups (NNMi Administrators, NNMi Level 2 Operators, NNMi Level 1 Operators, or NNMi Guest Users). This membership determines what you can see and do within the NNMi console.

## NNMi User Group

NNMi User Groups are those User Groups provided by NNMi. Users cannot access the NNMi console until their User Account is mapped to at least one of the following NNMi User Groups: NNMi Administrators, NNMi Level 2 Operators, NNMi Level 1 Operators (with less access privileges than Level 2 Operators), and NNMi Guest Users

## O

---

### OSPF

Open Shortest Path First Protocol

## P

---

### PE

Provider Edge router. The Internet Service Provider's router that receives your data on the path to your data's final destination. The Customer Edge (CE) router in your network connects to this PE.

### private IP addresses

These are IPv4 addresses that can be reused in home and office local area networks (LANs). Following the standards set by RFC 1918 and RFC 4193 (10.\*.\*.\*, 169.254.\*.\*, 172.16-31.\*.\*, and 192.168.\*.\*)

## R

---

### RAMS

HP Router Analytics Management System

### routing prefixes

A network protocol technique used to shorten or filter the amount of required routing information in each packet by declaring a prefix for an entire group of packets. This prefix also indicated the number of bits in the address.

## S

---

### SHA

Secure Hash Algorithm

## U

---

### unique local address

(fd00:: to fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff) A privately routable IPv6 unicast address used only for communication between nodes within your organization. The unique local addresses cannot be routed to the public internet. The address consists of a routing prefix in the fd00:/8 address spaces, assigned locally by your organization. And the full host address might be manually configured or automatically assigned using IPv6 auto-configuration and neighbor discovery.

### Unmanaged

Indicates the Management Mode is "Not Managed" or "Out of Service".

### UUID

Universally Unique Object Identifier, which is unique across all databases.



**V**

---

**VRRP**

Virtual Router Redundancy Protocol

