Hewlett Packard
Enterprise

HPE Network Node Manager i Software

Software Version: 10.20
for the Windows® and Linux® operating systems

Online Help: Help for Operators

Document Release Date: June 2016
Software Release Date: June 2016

Legal Notices

Warranty

The only warranties for HPE 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. HPE 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 HPE 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 2008–2016 Hewlett Packard Enterprise Development LP

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Apple is a trademark of Apple Computer, Inc., registered in the U.S. and other countries.

AMD is a trademark of Advanced Micro Devices, Inc.

Google™ is a registered trademark of Google Inc.

Intel®, Intel® Itanium®, Intel® Xeon®, and Itanium® are trademarks of Intel Corporation in the U.S. and other countries.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Internet Explorer, Lync, Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

Red Hat® Enterprise Linux Certified is a registered trademark of Red Hat, Inc. in the United States and other countries.

sFlow is a registered trademark of InMon Corp.

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 Visigoth Software Society (http://www.visigoths.org/).

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:
https://softwaresupport.hp.com

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:
https://hpp12.passport.hp.com/hppcf/createuser.do

Or click the **Register** link at the top of the HP Software Support 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: **https://softwaresupport.hp.com**

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:

https://hpp12.passport.hp.com/hppcf/createuser.do

To find more information about access levels, go to:

https://softwaresupport.hp.com/web/softwaresupport/access-levels

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is
http://h20230.www2.hp.com/sc/solutions/index.jsp

About this 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. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Chapter 1: Using Network Node Manager i Software (NNMi) 15
Node and Incident Access 15
Change Your Password 16

Chapter 2: Getting Started with NNMi (for Operators) 17
Best Practices Tour for the Incident Management Workspace 18
Best Practices Tour for the Topology Maps Workspace 21
Best Practices Tour for the Monitoring Workspace 23
Best Practices Tour for the Troubleshooting Workspace 24
Best Practices Tour for the Inventory Workspace 25
Best Practices Tour for the Management Mode Workspace 26
Best Practices Tour for the Incident Browsing Workspace 27

Chapter 3: NNMi's Global Network Management Feature (NNMi Advanced) 29
Is the Global Network Management Feature Enabled (NNMi Advanced)? 30
View the NNMi Management Servers' Domain List (NNMi Advanced) 31

Chapter 4: Learning Your Network Inventory 33
About Network Objects 33
Filter Views by Node or Interface Group 37
Nodes View (Inventory) 38
Interfaces View (Inventory) 39
IP Addresses View (Inventory) 41
SNMP Agents View 42
Web Agents View 43
IP Subnets View (Inventory) 43
VLANs View (Inventory) 44
Chassis View 45
Cards View 46
Ports View 46
Node Sensors View 47
Physical Sensors View 47
Layer 2 Connections View (Inventory) 48
Nodes by Management Server View (Inventory) 48
Nodes (All Attributes) View (Inventory) 49
Interfaces (All Attributes) View (Inventory) 50
IP Addresses (All Attributes) View (Inventory) 51
MIB Variables View (Inventory) 52
Chassis Redundancy Groups View (Inventory) 53
Card Redundancy Groups View (Inventory) 53
Router Redundancy Group View 54
Router Redundancy Members View (Inventory) (NNMi Advanced) 55
Node Groups View (Inventory) 56

Interface Groups View (Inventory) ... 56
Performance Analysis with Additional Views ... 57
Node Performance Metrics ... 57
Interface Performance Metrics ... 59
MPLS WAN Clouds (RAMS) View (NNMi Advanced) ... 61

Chapter 5: Accessing Device Details ... 62
Node Form ... 65
Node Form: General Tab ... 73
Node Form: IP Addresses Tab ... 76
Node Form: Interfaces Tab ... 76
Node Form: Virtual Switches Tab ... 77
Node Form: Chassis Tab ... 77
Node Form: Cards Tab ... 78
Node Form: Ports Tab ... 78
Node Form: VLAN Ports Tab ... 79
VLAN Port Form ... 79
Node Form: Router Redundancy Group Tab (NNMi Advanced) ... 80
Node Form: Capabilities Tab ... 80
Node Capabilities Provided by NNMi ... 81
Node Capability Form ... 83
Node Form: Node Groups Tab ... 84
Node Form: Node Sensors Tab ... 84
Node Form: Hosted Nodes Tab ... 86
Node Form: Custom Attributes Tab ... 87
Custom Node Attributes Form ... 87
Custom Node Attribute Samples ... 88
Node Form: Custom Polled Instances Tab ... 89
Node Form: Diagnostics Tab ... 91
Node Diagnostic Results Form (Flow Run Result) ... 91
Node Form: Incidents Tab ... 93
Node Form: Status Tab ... 93
Node Form: Conclusions Tab ... 95
Node Form: Scheduled Outage Tab ... 105
Node Form: Outage History Tab ... 105
Node Form: Registration Tab ... 106
Device Profile Form ... 107
Device Family Form ... 111
Device Vendor Form ... 111
Device Category Form ... 112
Interface Form ... 113
Interface Form ... 113
Interface Form: General Tab ... 118
Interface Form: IP Addresses Tab ... 120
Interface Form: Ports Tab ... 120
Interface Form: VLAN Ports Tab ... 121
Interface Form: Link Aggregation Tab (NNMi Advanced) ... 121
Interface Form: Performance Tab (NNM iSPI Performance for Metrics) ... 125

Interface Form: IP Addresses Tab 127
Interface Form: Capabilities Tab 128
Interface Capabilities Provided by NNMi 128
Interface Capability Form 134
Interface Form: Custom Attributes Tab 134
Custom Interface Attributes Form 135
Custom Interface Attribute Samples 136
Interface Form: Interface Groups Tab 136
Interface Form: Performance Tab (NNM iSPI Performance for Metrics) 137
Interface Form: Incidents Tab 139
Interface Form: Status Tab 140
Interface Form: Conclusions Tab 141
Interface Form: Registration Tab 154
Virtual Switch's Interface Form (NNMi Advanced) 155
Interface Form: Uplinks Tab (NNMi Advanced) 159
Interface Form: Virtual Ports Tab (NNMi Advanced) 160
IP Address Form 160
IP Address Form: Incidents Tab 163
IP Address Form: Capabilities Tab 163
IP Address Capabilities Provided by NNMi 164
IP Address Capability Form 165
IP Address Form: Status Tab 166
IP Address Form: Conclusions Tab 167
IP Address Form: Registration Tab 168
SNMP Agent Form 168
SNMP Agent Form: Status Tab 176
SNMP Agent Form: Conclusions Tab 177
SNMP Agent Form: Incidents Tab 180
SNMP Agent Form: Registration Tab 180
Web Agent Form (NNMi Advanced) 181
Web Agent Form: Device Credentials Tab (NNMi Advanced) 184
Web Agent Form: Managed Nodes Tab (NNMi Advanced) 184
Web Agent Form: Incidents Tab (NNMi Advanced) 185
Web Agent Form: Status Tab (NNMi Advanced) 185
Web Agent Form: Conclusions Tab (NNMi Advanced) 186
Web Agent Form: Registration Tab (NNMi Advanced) 187
Web Agent Form: Trusted Certificates Tab (NNMi Advanced) 188
Stored Agent Certificate Form (NNMi Advanced) 188
IP Subnet Form 189
IP Subnet Form: IP Addresses Tab 190
IP Subnet Form: Registration Tab 190
VLAN Form 191
VLAN Form: Ports Tab 193
Chassis Form 193
Chassis Form: General Tab 199
Chassis Form: Ports Tab 199
Chassis Form: Child Components Tab 200
Chassis Form: Hosted Nodes Tab 200

Chassis Form: Capabilities Tab ... 201
Chassis Capabilities Provided by NNMi ... 201
Physical Component Capability Form (Chassis) ... 202
Chassis Form: Custom Attributes Tab ... 203
Physical Component Custom Attribute Form (Chassis) ... 203
Chassis Form: Physical Sensors Tab ... 204
Chassis Form: Node Sensors Tab ... 205
Chassis Form: Incidents Tab ... 205
Chassis Form: Status Tab ... 206
Physical Component Status History Form (Chassis) ... 207
Chassis Form: Conclusions Tab ... 208
Physical Component Status Conclusions Form (Chassis) ... 210
Chassis Form: Registration Tab ... 210
Card Form ... 211
Card Form: General Tab ... 217
Card Form: Ports Tab ... 218
Card Form: Child Components Tab ... 218
Card Form: Hosted Nodes Tab ... 218
Card Form: Capabilities Tab ... 219
Card Capabilities Provided by NNMi ... 219
Physical Component Capability Form (Card) ... 220
Card Form: Custom Attributes Tab ... 221
Physical Component Custom Attribute Form (Card) ... 221
Card Form: Physical Sensors Tab ... 222
Card Form: Node Sensors Tab ... 223
Card Form: Incidents Tab ... 224
Card Form: Status Tab ... 224
Physical Component Status History Form (Card) ... 225
Card Form: Conclusions Tab ... 226
Physical Component Status Conclusions Form (Card) ... 228
Card Form: RegistrationTab ... 229
Port Form ... 229
Port Form: VLANs Tab ... 231
Port Form: RegistrationTab ... 231
Node Sensor Form ... 232
Node Sensor Form: Monitored Attributes Tab ... 235
Node Sensor Monitored Attribute Form ... 235
Node Sensor Form: Physical Components Tab ... 237
Node Sensor Form: Incidents Tab ... 237
Node Sensor Form: Status Tab ... 238
Node Sensor Status History Form ... 239
Node Sensor Form: Conclusions Tab ... 240
Node Sensor Status Conclusion Form ... 243
Node Sensor Form: Registration Tab ... 243
Physical Sensor Form ... 244
Physical Sensor Form: Monitored Attributes Tab ... 246
Physical Sensor Monitored Attribute Form ... 247
Physical Sensor Form: Incidents Tab ... 249

Physical Sensor Form: Status Tab ... 249
Physical Sensor Status History Form ... 250
Physical Sensor Form: Conclusions Tab ... 251
Physical Sensor Status Conclusions Form ... 254
Physical Sensor Form: Registration Tab ... 254
Layer 2 Connection Form ... 255
Layer 2 Connection Form: Interfaces Tab ... 257
Layer 2 Connection Form: Incidents Tab ... 258
Layer 2 Connection Form: Status Tab ... 258
Layer 2 Connection Form: Conclusions Tab ... 260
Layer 2 Connection Form: Link Aggregation Tab (NNMi Advanced) ... 265
Layer 2 Connection Form: Registration Tab ... 269
Chassis Redundancy Group Form ... 270
Chassis Redundancy Group Form: Redundant Components Tab ... 270
Chassis Redundancy Group Form: Incidents Tab ... 271
Chassis Redundancy Group Form: Status Tab ... 271
Chassis Redundancy Group Status History Form ... 272
Chassis Redundancy Group Form: Conclusions Tab ... 272
Card Redundancy Group Form ... 274
Card Redundancy Group Form: Redundant Components Tab ... 275
Card Redundancy Group Form: Incidents Tab ... 276
Card Redundancy Group Form: Status Tab ... 276
Card Redundancy Group Status History Form ... 277
Card Redundancy Group Form: Conclusions Tab ... 277
Router Redundancy Group Form (NNMi Advanced) ... 279
Router Redundancy Group Form: Router Redundancy Members Tab (NNMi Advanced) ... 281
Router Redundancy Member Form (NNMi Advanced) ... 281
Router Redundancy Member Form: Tracked Objects Tab (NNMi Advanced) ... 284
Tracked Objects Form (NNMi Advanced) ... 285
Router Redundancy Group Form: Virtual IP Addresses Tab (NNMi Advanced) ... 286
Virtual IP Addresses Form (NNMi Advanced) ... 287
Router Redundancy Group Form: Incidents Tab (NNMi Advanced) ... 287
Router Redundancy Group Form: Status Tab (NNMi Advanced) ... 287
Router Redundancy Group Status History Form (NNMi Advanced) ... 288
Router Redundancy Group Form: Conclusions Tab (NNMi Advanced) ... 289
Router Redundancy Group Form: Registration Tab (NNMi Advanced) ... 292
Node Group Form ... 293
Node Group Form: Device Filters Tab (NNMi Administrators only) ... 294
Node Device Filter Form (NNMi Administrators only) ... 295
Node Group Form: Additional Filters Tab (NNMi Administrators only) ... 296
Node Group Form: Additional Nodes Tab (NNMi Administrators only) ... 297
Additional Node Form (NNMi Administrators only) ... 297
Node Group Form: Child Node Groups Tab (NNMi Administrators only) ... 298
Node Group Hierarchy (Child Node Group) Form (NNMi Administrators only) ... 299
Node Group Form: Status Tab ... 300
Interface Group Form ... 302
Interface Group Form: ifType Filters Tab ... 303
ifType Filter Form ... 304

ifType (Interface Type) Form ... 304
Interface Group Form: Additional Filters Tab ... 305
MPLS WAN Cloud (RAMS) Form (NNMi Advanced) ... 305
MPLS WAN Cloud (RAMS) Form: MPLS WAN Connections Tab (NNMi Advanced) ... 306
Custom Node Collections Form ... 307
Custom Node Collections Form: Incidents Tab ... 309
Custom Node Collections Form: Status Tab ... 309
Custom Node Collections Form: Conclusions Tab ... 310
Custom Node Collections Form: Polled Instances Tab ... 311
Custom Polled Instance Form ... 312
Custom Polled Instance Form: Incidents Tab ... 315
Custom Polled Instance Form: Status Tab ... 315
Custom Polled Instance Form: Conclusions Tab ... 316
Custom Polled Collection Form ... 317
Comparison Map Form ... 320

Chapter 6: Scheduling Outages for Nodes or Node Groups ... 322

Chapter 7: Exploring SNMP MIB Source Information ... 326
MIB Form ... 326
MIB Form: MIB Variable Tab ... 327
MIB Variable Form ... 329
MIB Variable Form: Enumerated Values Tab ... 332
MIB Variable: Enumerated Values Form ... 332
MIB Variable Form: Table Indices Tab ... 334
Table Index Form ... 335
MIB Form: MIB Notifications Tab ... 337
MIB Notification Form ... 337
MIB Notification Form: Notification Variables Tab ... 339
Notification Variable Form ... 340
MIB Form: Textual Conventions Tab ... 342
Textual Convention Form ... 342
Textual Convention Form: Enumerated Values Tab ... 344
Textual Convention: Enumerated Values Form ... 344
Display a MIB File (source text file) ... 346
Determine which MIBs a Specific Node Supports ... 347

Chapter 8: Using the MIB Browser ... 348
MIB Browser Prerequisites ... 350
Run SNMP Walk Commands (MIB Browser) ... 351
Run SNMP Set Commands (MIB Browser) ... 356
Use Aliases in MIB Browser Commands ... 360
View MIB Browser Results ... 361
Save MIB Browser Results to a CSV File ... 363
Print MIB Browser Results ... 364

Chapter 9: Viewing Maps (Network Connectivity) ... 366
Node Group Maps ... 368

Navigating within a Node Group Map 370
Position Nodes on a Node Group Map 372
Add Annotations to a Map 372
Node Group Overview Map 374
Initial Discovery Progress or Network Overview Map 375
Networking Infrastructure Devices Map 376
Routers Map 377
Switches Map 378
Display the Layer 2 Neighbor View 378
Display the Layer 3 Neighbor View 381
Path Between Two Nodes that Have IPv4 Addresses 382
Path Calculation Rules 385
Path View Limitations 387
Investigate Errors and Performance Issues 388
MPLS WAN Cloud Map (NNMi Advanced) 389
Enhanced Path View (NNMi Advanced) 390

Chapter 10: Monitoring Devices for Problems 392
Monitor with Table Views 392
Non-Normal Node Sensors View 393
Non-Normal Physical Sensors View 394
Non-Normal Chassis View 395
Non-Normal Cards View 396
Non-Normal Interfaces View 396
Non-Normal Nodes View 397
Non-Normal SNMP Agents View 399
Not Responding Addresses View 399
Interface Performance View 400
Chassis Redundancy Groups View (Monitoring) 401
Card Redundancy Groups View (Monitoring) 401
Router Redundancy Group View 402
Node Groups View (Monitoring) 403
Custom Node Collections View 403
Custom Polled Instances View 404
Monitor with Map Views 405
Watch Status Colors 406
Determine Problem Scope 408
Access a Problem Device 408
Access Node Details 409
Access All Related Incidents 411
Export Maps to Microsoft® Visio 412
View the Details for a Map Object on an Exported Visio Diagram 414
Print an Exported Visio Diagram 414
Monitor with Graphs 415
Using Line Graphs 416
Display a Line Graph from an Incident (Custom Poller Only) 417
Display a Line Graph for a Custom Polled Instance 418
Change the Lines Displayed on a Line Graph 418

Emphasize a Line Displayed on a Line Graph 420
Hide a Line Displayed on a Line Graph 420
Display Messages on a Line Graph 421
Show and Hide the Line Graph Legend 422
Line Graphs Provided by NNMi 422
Using Stacked Area Graphs 424
Change the Stacked Areas Displayed on a Graph 424
Emphasize a Stacked Area Displayed on a Graph 426
Hide Data Displayed on a Stacked Area Graph 426
Display Messages on a Stacked Area Graph 427
Show and Hide the Stacked Area Graph Legend 428
Change the Polling Interval for a Graph 429
Select a Time Segment Using the Timeline Viewer 429
Unlock the Y-Axis When Viewing a Time Segment 430
Change the Zoom Value for a Graph 431
Display Data Values on a Graph 431
Determine the Maximum Time Range for a Graph 432
Print a Graph 433
Export Graph Data to a Comma-Separated Values (CSV) File 433

Chapter 11: Monitoring Incidents for Problems 435
Organize Your Incidents 437
Incident Form 437
Incident Form: General Tab 440
Incident Form: Correlated Parents Tab 446
Incident Form: Correlated Children Tab 446
Incident Form: Custom Attributes Tab 446
Custom Incident Attribute Form 447
Custom Incident Attributes Provided by NNMi (Information for Operators) 448
Incident Form: Diagnostics Tab 454
Incident Diagnostic Results Form (Flow Run Result) 454
Incident Form: Registration Tab 455
Manage Incident Assignments 456
Own Incidents 457
Assign Incidents 458
Unassign Incidents 459
Keep Your Incidents Up to Date 460
About the Incident Lifecycle 461
Track an Incident's Progress 461
Display a Map from an Incident 463
Island Node Group Map 464
Apply an Action to an Incident Source Node or Source Object 464
Monitor Incidents in a Global Network Management Environment (NNMi Advanced) 466
Incident Views Provided by NNMi 466
My Open Incidents View 468
Key Incident Views 468
Open Key Incidents View 470
Unassigned Open Key Incidents View 471

Closed Key Incidents View 472
Root Cause Incidents 473
Open Root Cause Incidents View 474
Service Impact Incidents View 475
All Incidents View 475
Custom Open Incidents View 476
Custom Incidents View 477
Syslog Messages View (HPE ArcSight) 478
SNMP Traps View 479

Chapter 12: Investigate and Diagnose Problems 480
Use a Dashboard View 482
Use the Analysis Pane 482
Verify Device Configuration Details 485
View the Monitoring Settings Report 486
Verify Current Status of a Device 488
Interpret Root Cause Incidents 490
Address Not Responding 491
Aggregator Interface Degraded (NNMi Advanced) 492
Aggregator Interface Down (NNMi Advanced) 493
Aggregator Connection Degraded (NNMi Advanced) 495
Aggregator Connection Down (NNMi Advanced) 496
All Cards Down in Chassis 497
Backplane is Out of Configured Range 498
Buffer has Insufficient Capacity or is Malfunctioning 500
Card Disabled 500
Card Down 501
Card Undetermined State 503
Cards Down in Chassis 504
Chassis Disabled 505
Chassis Down 506
Connection Down 507
CPU Utilization is too High 508
Custom Polled Instance in Collection is Out of Range 509
Fan is Out of Range or Malfunctioning 510
Interface Down 512
Interface Disabled 513
IP Subnet Contains IP with New MAC Address 514
Memory has Insufficient Capacity or is Malfunctioning 515
Node or Connection Down 515
Node Paused (NNMi Advanced) 517
Node Powered Down (NNMi Advanced) 517
Power Supply is Out of Range or Malfunctioning 518
Node Down 519
Remote Site Unreachable 522
Stack Degraded (NNMi Advanced) 522
Stack with no Slave (NNMi Advanced) 523
SNMP Agent Not Responding 524

Temperature Sensor is Out of Range 526
Voltage is Out of Range 527
Web Agent Not Responding (NNMi Advanced) 528
Interpret Incidents Related to SNMP Traps 529
Hosted Object Trap Storm 530
Message Queue Incident Rate Exceeded (NNMi Advanced) 531
Message Queue Size Exceeded (NNMi Advanced) 532
Pipeline Queue Size Exceeded Limit 533
SNMP Trap Limit (Warning, Major or Critical) 533
Trap Storm 534
Interpret Informational Incidents 535
Card Removed 535
Card Inserted 536
Node Deleted 537
Interpret Service Impact Incidents 537
Multiple Primary Cards in Card Redundancy Group 538
Multiple Primary Devices in Router Redundancy Group (NNMi Advanced) 539
Multiple Secondary Devices in Router Redundancy Group (NNMi Advanced) 539
No Primary Card in Card Redundancy Group 540
No Primary Device in Router Redundancy Group (NNMi Advanced) 541
No Secondary Card in Card Redundancy Group 542
No Secondary Device in Router Redundancy Group (NNMi Advanced) 543
Primary Device in Router Redundancy Group Switched (NNMi Advanced) 543
Router Redundancy Group Degraded (NNMi Advanced) 544
Interpret Threshold Incidents 545
Backplane Incidents (NNM iSPI Performance for Metrics) 548
Buffer Incidents (NNM iSPI Performance for Metrics) 550
CPU Incidents (NNM iSPI Performance for Metrics) 552
Disk Incidents (NNM iSPI Performance for Metrics) 554
Interface Frame Check Sequence (FCS) Error Rate Incidents (NNM iSPI Performance for Metrics) 556
Interface Input and Output Discard Rate Incidents (NNM iSPI Performance for Metrics) 557
Interface Input and Output Error Rate Incidents (NNM iSPI Performance for Metrics) 559
Input and Output Queue Drop Incidents (NNM iSPI Performance for Metrics) 560
Interface Input and Output Utilization Incidents (NNM iSPI Performance for Metrics) 562
Management Address ICMP Response Time Incidents 565
Memory Incidents (NNM iSPI Performance for Metrics) 567
Find a Node 569
Find the Attached Switch Port 571
Display End Nodes Attached to a Switch 573
Test Node Access (Ping) 575
Find the Route (traceroute) 577
Establish Contact with a Node (Telnet or Secure Shell) 578
Check Status Details for a Node Group 579

Chapter 13: Viewing Lists of the Unmanaged Objects in Your Network 581
Unmanaged Nodes View 581
Unmanaged Interfaces View 582

Unmanaged IP Addresses View 583
Unmanaged Chassis View 583
Unmanaged Cards View 584
Unmanaged Node Sensors View 585
Unmanaged Physical Sensors View 585
Scheduled Node Outages View 586
Stop or Start Managing an Object 587
Understand the Effects of Setting the Management Mode to Not Managed or Out of Service 589
How NNMi Assigns the Management Mode to an Object 591
How NNMi Users Change a Management Mode 592

Chapter 14: Checking the Status of NNMi 594
Hide Connections or Connection Labels from an Exported Visio Diagram 594

Glossary 596

Send Documentation Feedback 601

Chapter 1: Using Network Node Manager i Software (NNMi)

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 392 and "Investigate and Diagnose Problems" on page 480
Annotate information for future diagnosis	"Accessing Device Details" on page 62
Look for historical information to proactively monitor the network	"Monitoring Incidents for Problems" on page 435
View an inventory of what is being managed	"Learning Your Network Inventory" on page 33
Change your password	"Change Your Password" on the next page
Check NNMi health	"Checking the Status of NNMi" on page 594

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 and 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.

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**[1], 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.

   Type any amount of printable alpha-numeric characters or symbols.
4. In the **Confirm Password** attribute, retype your new password.
5. Click **OK**.

[1]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: Getting Started with NNMi (for Operators)

Welcome to Network Node Manager i Software (NNMi) — NNMi automates many network management tasks, making your job easier.

For information about using the NNMi console, see About the NNMi Console and Navigating the NNMi Console. For information about using the online help, see Access Help and Search the Help Topics.

The following Best Practices Tours explain some of NNMi's capabilities that help you keep the network up and running. These tours are organized by task and the associated NNMi console workspace.

Task	NNMi Console Workspace
Determine the following: • For which devices are you responsible (Nodes and Node Groups)? • Which of those devices would cause the most disruption in network traffic if anything goes wrong?	Topology Maps
Quickly identify problem devices (Nodes) in your network environment. View information about a selected set of devices (Node Group).	Inventory
View the incident history for one or more problems. **Tip:** NNMi generates incidents to proactively alert your team about potential problems or actual problems.	Incident Browsing
Take action on an incident that alerted you to a problem with one or more devices.	Incident Management
• Determine the location or context of the problem. • Ascertain the health of a particular network device or Node Group. • Check the real-time routing path between nodes.	Troubleshooting
Proactively monitor the health of one or more devices in your network environment.	Monitoring
• Identify nodes scheduled for maintenance or a scheduled outage. • Prevent incidents from being generated for one or more objects.	Management Mode

For detailed information about these tasks and many other NNMi topics, see:

- **Help → Using the NNMi Console**
- **Help → Help for Operators**

Best Practices Tour for the Incident Management Workspace

This Best Practices Tour describes how to use the **Incident Management** workspace to take action on incidents assigned to you and your team. The views in this workspace display any information that the NNMi administrator allows you to see.

The **Incident Management** workspace, contains the following views:

- **Open Key Incidents** table view

  By default this table view lists the types of incidents described in the following table and is filtered to show only those incidents with a Severity that is *not Normal* (Critical, Major, Minor, or Warning). You can change the Severity Filter (or any column filter) by right-clicking the column of interest.

Incident Correlation Nature	Description
Info	This Correlation Nature is meant to be informational.
None	Indicates there is no incident correlation for this incident.
Rate Stream Correlation	Indicates the incident tracks incident patterns *based on the number of incident reoccurrences within a specified time period*. 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.
Root Cause	Indicates an incident that NNMi's Causal Engine determined to be the root cause of a problem.
User Root Cause	Indicates that your NNMi administrator configured NNMi to always treat this Incident as Correlation Nature: Root Cause.

  Note: Key Incidents do not include Incidents with following Correlation Natures because they are not considered to be Key Incidents:

  Dedup Stream Correlation

  Secondary Root Cause

  Symptom

- **Unassigned Open Key Incidents** table view

  This view displays all incidents that do not have any owner. To own an incident, click the incident row of interest, and then select **Actions** → **Assign** → **Own Incident**. To assign the incident to someone else, select **Actions** → **Assign Incident**. In the **Assign Incident** dialog select the name of the User Account to which you want to assign the incident and click **OK**.

- **My Open Incidents** table view

NNMi displays the incidents assigned to your User Account. These incidents are the incidents that likely require the most immediate attention from you.

Incidents originate from a variety of sources:

- SNMP Traps generated from SNMP agents on managed devices in your network environment. Note that many SNMP traps never become incidents (the NNMi administrator must configure that to happen for each trap definition).
- Incidents that your NNMi Administrator configured so that NNMi notifies the team when a specific issue is detected.
- Incidents generated as a result of other incidents. NNMi analyzed the available data and arrived at a *Conclusion*that indicates some problem needs to be addressed. See **Help → Help for Operators**, and use Search to find the following text string including quotes `"outstanding status conclusions"` to find the complete list of all conclusions for each managed object.

Solve Network Problems

1. 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 Sensors (such as CPU and memory)
   - Interface
   - IP Address
   - Chassis and its Physical Sensors (such as backplane and fan)
   - Card
   - SNMP Agent
   - Node Group
   - Card Redundancy Group
   - Router Redundancy Group
2. 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.
3. 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.

4. 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 yow with identifying the problem.
5. Select the **Actions** menu to explore additional troubleshooting choices:

   Note: Access to these commands depends on the **NNMi Role**[1] and Object Access Privileges to which you are assigned. If you are unable to access an action, contact your NNMi administrator.

   - Use **Maps** to see the location of the node, and its connections to (communication channels with) other devices.

     Maps are a quick way to determine the nodes that have a Status other than *Normal*. Maps are also a valuable tool that helps you determine the scope of a problem. For example, a map can indicate whether the problem affects an entire site or only a small subset of devices. The map view you select depends on the types of information you want to view.
     - **Maps** → **Node Group** map displays the group of nodes, if any, to which the selected node belongs. Your NNMi administrator can configure Node Groups that group nodes together according to selected criteria. For example, nodes grouped by location, importance, or device type.
     - **Maps** → **Path View** is a flow diagram rather than a connection diagram. It displays the flow of network traffic between two devices, 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.
   - Use the **Graphs** submenu to monitor one or more devices in real-time. For example, if you receive a call that email is slow, you might want to view a line graph that monitors the utilization of the interfaces on the email server. To select a graph, first select the MIB file that contains the types of information you want to display.
   - Use the **Node Access** submenu when you want to check whether a node is reachable or to log on to the device.
   - Select either **Node Actions**, **Interface Actions**, or I**P Address** Actions and then use the **Polling** submenu when you suspect that NNMi is incorrectly reporting the status or configuration for a device:
     - **Polling** → **Status Poll** to force NNMi to repoll the device so that NNMi updates its Status and Discovery State (for example, NNMi reports that an interface is down, but you believe it is up).

[1]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.

- **Polling → Configuration Poll** to force a re-discovery of the device (for example, if you suspect that NNMi is missing an interface for the node).

- Select either **Node Actions**, **Interface Actions**, or I**P Address** Actions and then use the **Configuration Details** submenu when you want to check a device's Communication Configuration settings or Monitoring Configuration settings. Communication Configuration information includes SNMP and ICMP configuration values. Monitoring Configuration information includes the types of polling enabled, the fault and performance polling intervals, as well as the Management Mode for the selected node.

- Select **Node Actions** and then use the **MIB Information** submenu when you want to see the results of List Supported MIBs or to use the MIB Browser for determining more details about the object (by issuing SNMP MIB Walk or SNMP MIB Set commands).

- Select **Node Actions** and then use **Show Attached End Nodes** to determine the end nodes, if any, attached to a switch.

6. As another best practice, check the timing of the incident to determine whether the incidents coincides with a known network episode.

See "Best Practices Tour for the Incident Browsing Workspace" on page 27 when you want to filter on more possible patterns related to incidents.

Best Practices Tour for the Topology Maps Workspace

This Best Practices Tour describes how to use the **Topology Maps** workspace to determine which devices your NNMi administrator has assigned to you and your team. Each NNMi user might see a different set of views and of network devices within those views, depending on how your NNMi administrator configures NNMi.

Note: You will see some or all of the workspaces and views described, depending on several factors:

- Your assigned NNMi Security Group Mapping.
- The HPE Network Node Manager i Smart Plug-in software currently installed.
- Your NNMi administrator can integrate other applications into NNMi. Therefore, you might see things that are not described in the NNMi online help. Contact your NNMi administrator if you have questions about any additional items that are not described.

The Default View

When you first open the NNMi console, you might see the **Initial Discovery Progress** map. NNMi displays this map by default when it has discovered less than or equal to a total of 100 routers, switches, and switch-routers. This map displays the 100 devices in your network environment that generate Layer 3 traffic to the highest number of other devices in your network environment (routers, switches, and switch-routers). The map dynamically changes each time NNMi discovers additional nodes.

Your NNMi administrator can configure the default view. For example, you might see the **Network Overview** map each time you open the NNMi console. Your NNMi administrator also might have added maps to the Topology Maps workspace, in addition to those described here.

The Topology Maps Workspace

In the **Topology Maps** workspace, you will find the following maps if your NNMi administrator allows you to see them:

- **Node Group Overview** map

  This map provides a link to all the Node Groups your NNMi administrator configured for you and your team. Your NNMi administrator defines a set of criteria that determines the members of each Node Group. If you think of criteria for another useful group, be sure to tell your NNMi administrator about your ideas; for example, location, importance, or device type.

  To determine the members of a Node Group, double-click the six-sided Node Group icon of interest. Then, to access more details about one of the Node Group's members, double-click the icon of interest to access a node's form.

- **Network Overview** map

  This map displays the 250 devices in your network environment that can potentially generate Layer 3 traffic to the highest number of other devices in your network environment (routers, switches, and switch-routers). These 250 devices are connected to (communicating with) the highest number of other devices.

  - **Node Group** maps.
    - **Networking Infrastructure Devices** maps

      This map displays all of the following in your network environment, and the connections between those network devices:

      Note that each connection (line) can indicate any number of communication channels between those devices. A thick line represents multiple connections.

      Firewalls , Switches , Routers and Switch-Routers

      Nested beneath the Node Group Maps folder are all Node Group Maps that were saved by an NNMi user some time in the past (= saved. = not saved). The default list is:

      - **Routers** map

        This map displays all current members of the Routers Node Group, and all connections between those devices. Out-of-the-box, the Routers Node Group criteria includes Gateways, Routers, and Switch-Routers. (Your NNMi administrator might have changed this.)

      - **Switches** map

        This map displays all current members of the Switches Node Group, and all connections between those devices. Out-of-the-box, the Switches Node Group criteria is Switches and Switch-Routers. (Your NNMi administrator might have changed this.)

- **Quick Access Maps** folder contains all maps your NNMi Administrator configured to have an ordering number (which controls where in the list that map appears).
- **All Node Groups** folder is visible only to NNMi Administrators and shows a list of all Node Groups that have been defined.

Using the Topology Maps Workspace

Map symbols represent nodes or groups of nodes that were defined by the NNMi administrator. Each map symbol has a background shape and most have a superimposed foreground image. The background shape conveys the device type, and the foreground image can be used to represent specific vendors or models for that device. See About Map Symbols for more information. Communication channels between devices are depicted as lines on the map.

The color of the background shape of each map symbol conveys the most recent health status. The color of each line representing a connection (communication channel) conveys the most recent health status of that connection. For example, the color red (critical) indicates NNMi detected problems related to the associated object that requires immediate attention. The color yellow (minor) indicates NNMi detected problems related to the associated object that requires further investigation. The color orange (major) indicates NNMi detected problems related to the associated object that must be resolved before those issues become critical. See About Status Colors for a description of possible status colors.

If you single-click any map object, NNMi performs the appropriate analysis on the object and determines the most important related information to display. This information is displayed in the Analysis Pane (in the bottom half of the window). Any summary details for the selected object appear in the leftmost panel of the Analysis Pane.

If you double-click any map object, NNMi displays the selected object's form. The form includes a number of tabs containing all information NNMi knows about that object. For example, each node form contains information about the node's IP addresses, interfaces, cards, ports, associated incidents, and much more.

At the top of each map, your navigation choices become breadcrumbs that enable you to return to a previous location. For example, from a Node form, to return to the Node Group Overview map, click the **Node Group Overview** breadcrumb.

See the "Best Practices Tour for the Troubleshooting Workspace" on the next page for more information about using maps to proactively troubleshoot network problems.

Best Practices Tour for the Monitoring Workspace

This Best Practices Tour describes how to use the **Monitoring** workspace to determine the health of your network devices.

Use the **Monitoring** workspace to examine the node sensors, physical sensors, chassis, cards, interfaces, nodes, SNMP Agents, or addresses whose health is not Normal (Critical, Major, Minor, or Warning). This workspace also contains views for groups of card redundancy groups, router redundancy groups, and node groups whose health is not Normal.

The **Custom Node Collections** and **Custom Polled Instances** views are used when the NNMi administrator has configured device polling to include MIB variables that are not otherwise monitored by NNMi.

When you open a view in the **Monitoring** workspace, and select a row, the Analysis Pane displays in the bottom half of the window. NNMi performs analysis of the selected object and determines the most important information to display. Any Summary details for the selected object appear in the leftmost panel. This Summary panel provides a convenient way to access the form for any related objects. To explore information about the Node, 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).

To access a related object's form, click the row or hyperlink that represents the object of interest.

For detailed information on these and many other NNMi topics, see the **Help → Using the NNMi Console** and **Help → Help for Operators** from the NNMi console's toolbar.

Best Practices Tour for the Troubleshooting Workspace

This Best Practices Tour describes how to use the **Troubleshooting** workspace to troubleshoot network problems.

> **Tip:** The **Troubleshooting** workspace provides access to the same maps as the **Actions → Maps** submenu.

Use the maps in the **Troubleshooting** workspace to see the location of a node, its connections (communication channels) to other devices, and each node's Status color (calculated by NNMi based on all available data). Status values are listed in table views, as well as on maps. Possible Status values include:

Status	Map Symbol Background Color	Table Column Symbol
No Status		none
Normal		
Warning		
Minor		
Major		
Critical		
Disabled		
Unknown		

See Status Color for Objects and Status Color for Aggregator Objects (*NNMi Advanced*) for more information about Status colors and values.

NNMi uses SNMP and ICMP Polling to gather information about the health of each device in your network environment.

Maps are a quick way to determine which nodes have a Status that is not Normal (green). Maps are valuable tools that help you determine the scope of a problem. For example, a map can indicate whether a problem

affects an entire site or only a small subset of devices. The map view you select depends on the types of information you want to view.

The **Layer 2 Neighbor View** shows a graphical representation of the selected device and any connections with other devices within a specified number of hops (other devices) from the selected device. The map also shows the health of those devices. Layer 2 Connections traverse switches and switch-routers.

The **Layer 3 Neighbor View** is a graphical representation of the devices in subnets to which the selected node belongs, and the health of the routers in those subnets. The connections in this map traverse routers and switch-routers.

The **Node Group Map** displays the group of nodes, if any, to which the selected node belongs. Your NNMi administrator can configure Node Groups to group nodes together according to selected criteria, for example by location, importance, or device type.

A **Path View** map displays the flow of network traffic between two devices, rather than all of the available connections. Path View calculates the route of data flow between two nodes, and provides a map of that information. The end nodes can be Nodes or Routers.

To access the form for any object on the map, double-click the object of interest.

Tip: See also the `nnmtopoquery.ovpl` Reference Page. Use this command-line tool to list all connected neighbor interfaces for a specified node.

Best Practices Tour for the Inventory Workspace

This Best Practices Tour describes how to use the **Inventory** workspace to determine which nodes are having problems.

There are important differences between **Inventory** workspace views:

- The *(All Attributes)* table views (**Nodes (All Attributes)**, **Interfaces (All Attributes)**, and **IP Addresses (All Attributes)**) show all columns (attributes) available for the object type. Configure these views to meet your current need.
- The other table views display a pre-determined subset of columns (attributes).
- NNMi provides Inventory views for the following objects: Nodes, Interfaces, IP Addresses, SNMP Agents, IP Subnets, Virtual LANs, Chassis, Cards, Ports, Node Sensors, Physical Sensors, Layer 2 Connections, MIB Variables, Chassis Redundancy Groups, Card Redundancy Groups, Router Redundancy Groups, Router Redundancy Members, Node Groups, and Interface Groups.

Right-click a column heading in these table views to fine-tune the displayed data, based on any of the following criteria:

- **Select All** (to select all rows in the table)
- **Sort** (Ascending or Descending)
- **Filter** (choices vary from column to column)
- **Visibility** (to show/hide each available column)

Use NNMi's **Filter** option to group nodes without creating Node Groups. For example, filter all of the nodes in your **Nodes (All Attributes)** view by **Device Vendor** so that the view includes only Hewlett-Packard devices:

1. Right-click the **Device Vendor** column.
2. Select **Filter** → **Create Filter**.
3. Select **equals**.
4. Click **Hewlett-Packard**.
5. Click **OK** to save your changes.

   NNMi displays only those devices whose Device Vendor is Hewlett-Packard.

Tip: When you select an object, the Analysis Pane displays in the bottom half of the window .The Analysis Pane's Details tab includes a **System Description** attribute with the IOS version for any Cisco device. Each tab in the Analysis Pane provides you with more details about the selected object.

Best Practices Tour for the Management Mode Workspace

This Best Practices Tour describes how NNMi administrators and Level 2 Operators can use the Management Mode workspace for scheduled maintenance.

Each of the views in the **Management Mode** workspace provides a set of objects that currently have a Management Mode of either **Not Managed** or **Out of Service**:

Possible objects include nodes, interfaces, IP addresses, chassis, cards, node sensors (for example buffers. CPU, disks, memory), and physical sensors (for example backplane, fan, power, temperature, voltage). To view the list of possible attribute values for any table column in the view, right-click the column heading and select Filter. Then select Create Filter. NNMi displays each possible attribute value.

When the Management Mode is set to **Not Managed** or **Out of Service**, NNMi stops polling the specified object and no incidents are generated. Use **Not Managed** when you want to stop managing a node for reasons other than scheduled maintenance. Use **Out of Service** for those nodes that are temporarily out of service. See "Understand the Effects of Setting the Management Mode to Not Managed or Out of Service" on page 589.

To set the Management Mode for an object:

1. Navigate to the view of interest (for example **Nodes** view under the **Inventory** workspace).
2. Double-click the row representing the object of interest.
3. In the object form, navigate to the Management Mode drop-down list and select the new Management Mode:
   - When you select the **Not Managed** or **Out of Service** Management Mode, NNMi adds the object to the Management Mode view for that object type. See "Stop or Start Managing an Object" on page 587 and "How NNMi Users Change a Management Mode" on page 592.

     Tip: Remember to reconfigure the Management Mode of those objects that are no longer out of service. To do so, double-click the row representing the object of interest and reset the

Management Mode to **Managed**.

- You can also schedule a time for NNMi to automatically change the management mode to **Out of Service** for a specific time period. See "Scheduling Outages for Nodes or Node Groups" on page 322.

Best Practices Tour for the Incident Browsing Workspace

This Best Practices Tour explains how to use the **Incident Browsing** workspace to research an issue you are trying to resolve in your network environment.

The **Incident Browsing** workspace contains nine views. You can Filter these views by time period, Node Group, or any column's data (by right-clicking on the column heading):

- Sort the data.
- Filter the data.
- Show or Hide columns (Visibility).

Select any table row and click the **Actions** menu to see what (if anything) you can do with each incident.

There are important differences between **Incident Browsing** workspace views:

- The custom table views (**Custom Open Incidents** and **Custom Incidents**) show all incidents and all columns (attributes). Configure these views to meet your current need. Note that due to potential performance concerns with large lists, this view is not automatically Refreshed.
- Other table views show a pre-filtered list of incidents and display a pre-determined subset of columns (attributes) according the view's title text.

The following pre-configured views contain lists of incidents that most likely require immediate attention:

- **Open Key Incidents** lists all of the Open Root Cause Incidents and Service Impact incidents whose Severity is *not Normal* (Critical, Major, Minor, or Warning). The following two views are subsets of the data in this view.
- **Open Root Cause Incidents** lists all incidents (any Severity) that NNMi determines are the cause of or source of a problem. Any incidents in this view with a Severity other than Normal also appear in the Open Key Incidents view.
- **Service Impact Incidents** lists all incidents (any Severity) that NNMi determines might impact a related application in your network environment. Any incidents in this view with a Severity other than Normal also appear in the Open Key Incidents view.

The following pre-configured views provide lists that network management teams often find useful:

- **Closed Key Incidents** tracks the key incidents that have been resolved by your team or automatically resolved because of positive changes in the network environment.
- **All Incidents** lists all incidents generated by NNMi. Note that due to potential performance concerns with large lists, this view is not automatically Refreshed.
- **SNMP Traps** lists traps generated from SNMP agents on managed devices in your network environment. Note that many SNMP traps never become incidents (the NNMi administrator must configure that to happen for each trap definition). For example, if the NNMi administrator configures the SNMP Link Down

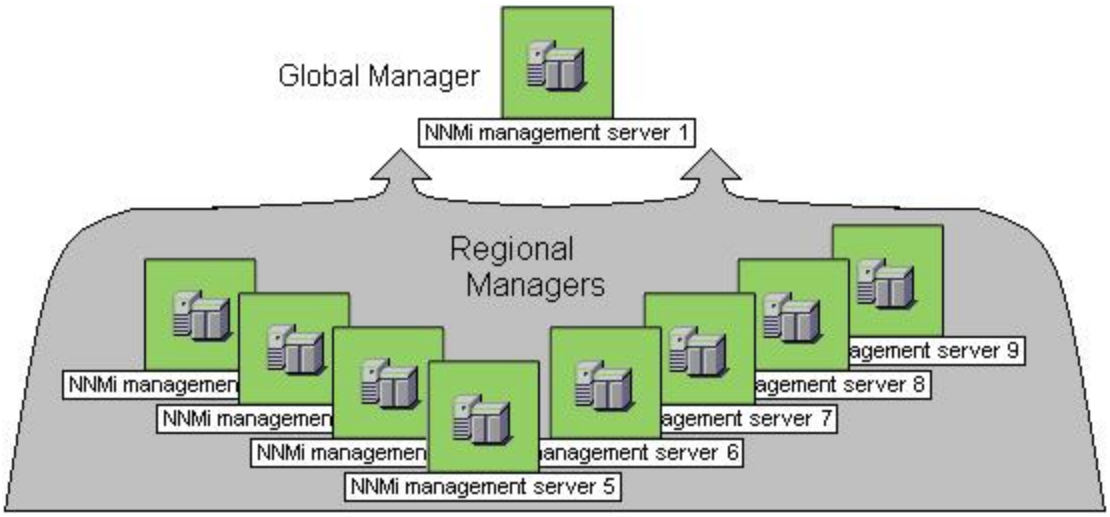
trap to generate a Root Cause incident, when you open the generated Interface Down incident, data about the related Link Down trap is listed on the Incident form's General tab.

Tip: To view the history of incidents for a particular node, select the incident and then select **Actions** → **Source Node**. NNMi opens the Node form. Navigate to the **Incidents** tab.

See "Best Practices Tour for the Incident Management Workspace" on page 18 for more information. Use the **Incident Management** workspace to take action on incidents assigned to you and your team.

Chapter 3: 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 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 466 .

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 48 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 38 for more information about this view.

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" on page 37 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.

Note: NNMi supports physical and virtual network objects. See "About Network Objects" below for more information.

For a short description of each Inventory view: Views Available in NNMi

About Network Objects

NNMi can monitor and analyze a variety of network devices and components within those devices. NNMi uses the SNMP protocol and the `ping` network administration utility to retrieve up-to-the-minute information. NNMi supports both physical and virtual (logical) devices.

The following list shows the specific network objects that NNMi monitors and analyzes. Click an object for more information.

Note: The following objects represent physical components:

- Cards
- Chassis

- Physical Sensors (backplane, fan, power supply, temperature gauge, and voltage regulator)
- Ports

The remaining items in the following list can be physical or virtual.

- **Aggregator Interfaces** (*NNMi Advanced*)

  An Aggregator Interfaces is a set of interfaces on a switch that are linked together, usually for the purpose of creating a trunk (high bandwidth) connection to another device. Aggregator Interfaces have designated Aggregation Member Interfaces.

- **Aggregator Layer 2 Connection** (*NNMi Advanced*)

  An Aggregator Layer 2 Connection is a connection with endpoints that are Aggregator Interfaces. These are usually high-bandwidth connections that link switches. Aggregator Layer 2 Connections have Aggregator Interfaces and Aggregation Members.

- **Cards**

  A card is a physical component on a device which generally has physical ports that contain one or more interfaces used to connect to other devices. A card can also contain sub-cards. The card containing another card is known in NNMi as the Parent Card. The sub-card is known as a Daughter Card. NNMi supports Daughter cards one level deep.

- **Card Redundancy Groups**

  A Card Redundancy Group is a set of card modules that are configured to provide card redundancy on the device. These cards are management modules on Cisco and HPEs Procurve platforms. The number of cards supported in a group on both platforms is two. The Card Redundancy Group has one card acting as the primary member, the other acting as the secondary. If the primary card fails, the secondary card takes over as the primary card.

- **Chassis**

  A Chassis is a physical component on a device into which other objects are plugged, such as cards. A Chassis can also contain sub-chassis. The Chassis containing another Chassis is known in NNMi as the Parent Chassis. The sub-chassis is known as the Child Chassis. A Child Chassis can be one-level deep.

  NNMi supports the following scenarios:

  - A single node running on one chassis
  - Multiple nodes running on one chassis
  - A single node running on multiple chassis

  Chassis are connected by Inter Switch Links (ISL). A port used for the Inter Switch Link is designated with the Type **IRF physical port** and is associated with the card or chassis on which it resides.

- **Chassis Redundancy Groups**

  A Chassis Redundancy Group is a set of chassis that are configured to provide redundancy (for example, for switches). Each redundancy group member is discovered as a Chassis managed by a node. Each Chassis Redundancy Group member has one of the following roles:

- Master - Indicates the chassis is the master member of the Chassis Redundancy Group.
- Slave - Indicates the chassis is a slave member of the Chassis Redundancy Group.

- **Field Replaceable Units (FRU Card)**

  A Field-Replaceable-Unit (FRU) card is a card that can be replaced on a device that is operationally active (not powered down). When an FRU card is removed from or added to the device, NNMi reports the occurrence with an incident. If an FRU card is not recognized by the device, NNMi reports the unrecognized card with an incident.

- **Interfaces**

  An interface is a logical object that might or might not be associated with a physical port. Interfaces are used to identify connections between nodes. Multiple interfaces can be associated with a single physical port. NNMi identifies interfaces using either of the following values:

  - ifName
  - ifAlias
  - ifType[ifIndex] (for example, ethernetCsmacd[17])

  Each physical port managed by NNMi is associated with one or more interfaces. NNMi identifies ports using the <*Card-number* / *Port-number*> value.

- **Interface Groups**

  An Interface Group is a logical collection of interfaces created by an NNMi administrator.

- **IP Addresses**

  An IP address is a routable address that responds to ICMP. IP addresses are typically associated with nodes.

- **IP Subnets**

  Identifies all of the networks within your management domain. Each IP Subnet represents an IP Subnet within a particular Tenant (that IPv4 Subnet definition independently applies to each Tenant).

- **Layer 2 Connections**

  Connections are Layer 2 physical connections and Layer 3 network connections. NNMi discovers connection information by reading forwarding database (FDB) tables from network devices and gathering data from a variety of Layer 2 *discovery protocols* (see the list of Topology Source protocols in Layer 2 Connection Form).

- **Nodes**

  A node is a device that NNMi finds as a result of the Spiral Discovery process. A node can contain interfaces, boards, and ports. You can separate nodes into two categories:

  - Network nodes, which are active devices such as switches, routers, bridges, and hubs

    Note: These nodes can be physical or virtual and can represent one or more additional objects,

such as a switch stack.

  - End nodes, such as Linux or Windows servers

- **Node Sensors**

  Some network devices enable SNMP Agents to monitor certain aspects of ongoing usage such as buffers, CPU utilization, disk utilization, and memory utilization. NNMi administrators can monitor the health of these by configuring node sensors to alert their team members when any of these aspects of operation are marginal or failing.

- **Node Groups**

  A Node Group is a logical collection of nodes created by an NNMi administrator.

- **Physical Sensors**

  Some network devices enable SNMP Agents to monitor internal components such as backplane, fan, power supply, temperature guage, and voltage regulator. NNMi administrators can monitor the health of these components by configuring physical sensors to alert their team members when any of these components operate marginally or fail.

- **Ports**

  Physical ports hosted on a card, used by a node that NNMi is monitoring.

- **Router Redundancy Groups** (*NNMi Advanced*)

  A Router Redundancy Group is a set of routers that are configured to provide redundancy in the network. Such groups use the following two types of protocols:

  - Hot standby router protocol (HSRP)
  - Virtual router redundancy protocol (VRRP)

  Router Redundancy Groups usually have a single device acting as the primary, a single device acting as a secondary, and any number of standby devices. If the primary device fails, the secondary device should take over as primary, and one of the standby devices should become secondary. The router groups employ either the HSRP or VRRP protocol to designate the primary, secondary, and standby routers.

- **Router Redundancy Members** (*NNMi Advanced*)

  Each router in the Router Redundancy Group.

- **SNMP Agents**

  An SNMP agent is a process interacting with the managed node and providing management functions. The SNMP agent is responsible for SNMP communications with the managed node. An SNMP Agent can be associated with one or more nodes.

- **VLANS**

  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.

Related Topics

The NNMi Causal Engine and Object Status

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.

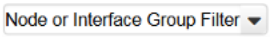
Node Group filters are available for:

- Node views
- Interface views
- IP address views
- Incident views
- Node Sensor views
- Physical Sensor views

Interface Group filters are available for:

- Interface views
- IP Address views
- Card 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 65 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 **Status** so that you can be quickly alerted to existing and potential problems.
View all device types being managed	Sort the view by the **Device Profile** attribute.
Identify whether the problem can be isolated to a particular area of your network	Sort the view by **System Location**. This is the current value of the sysLocation MIB variable.
View address and subnet information associated with a selected node to better determine the scope of the problem	From the **Nodes** view, open the **Node** form. Select the **Addresses** tab.
Access a map view of a selected node and its surrounding topology	Select the node of interest and use the **Actions** menu from the main toolbar to select either the Layer 2 or Layer 3 Neighbor View. See Using Table Views 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 **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.

Uses for Nodes Views, continued

Use	Description
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 Filter Information in a Table View for more information.
(*NNMi Advanced - Global Network Management feature*) If your NNMi management server is a Global Manager, identify which nodes are managed by each Regional Manager.	See "NNMi's Global Network Management Feature (NNMi Advanced)" on page 29 for more information. Sort the Node view using the NNMi Management Server column (at the far right of the view). 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.

Related Topics:

Using Table Views

"Node Form" on page 65

Export Table Information

Interfaces View (Inventory)

Tip: See "Interface Form" on page 113 for more details about the interface attributes that appear in this view's column headings.

The **Interfaces** view in the Inventory workspace 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, the date and time its status was last changed, the date and time its state was last changed, 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 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 **Hosted On Node**. 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 **Status** attribute.
Access a map view of the network interface and its surrounding topology.	Select the interface of interest and use the **Actions** menu to select either the Layer 2 or Layer 3 Neighbor view. See Using Table Views for more information.
View the status of all of the interfaces that	Your NNMi administrator can create nodes and interface

Uses for Interfaces Views, continued

Use	Description
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.	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 "Filter Views by Node or Interface Group" on page 37 for more information.

Related Topics:

Using Table Views

"Interface Form" on page 113

Export Table Information

IP Addresses View (Inventory)

Tip: See "IP Address Form" on page 160 for more information about the IP address attributes that appear in this view's column headings.

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

For each IP address displayed, you can identify its status, state, IP address, interface name (**In Interface**), associated node Name value (**Hosted On Node**), the subnet prefix (**In Subnet**) and prefix length (**PL**), the date and time its status was last changed, 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 **Hosted On Node** attribute.
View the addresses per interface	Sort the view on the Interface name (**In Interface**) attribute.
View the addresses per subnet	Sort the view on the subnet (**In Subnet**) attribute.
View the subnet information for a selected IP address	To access a subnet from this view: 1. Select the IP address of interest. 2. Open the **IP Address** form 3. Navigate to the **In Subnet** attribute. Click the Lookup

Uses for the IP Addresses View, continued

Use	Description
	icon and select Open to access the **IP Subnet** form.
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 "Filter Views by Node or Interface Group" on page 37 for more information.

Related Topics:

Use Table Views

"IP Address Form" on page 160

Export Table Information

SNMP Agents View

Tip: See "SNMP Agent Form" on page 168 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 (SNMP 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

Web Agents View

Tip: See "Web Agent Form (NNMi Advanced)" on page 181 for more details about the Web Agent attributes that appear in this view's column headings.

For each **Web Agent**[1] displayed in the view, you can view the following details:

- Status of the Web Agent
- Agent State
- Hosted on Node (device on which the Web Agent resides)
- Hostname (FQDN) of the host device
- Mode
- Agent Enabled
- Scheme (communication)
- Port (on which the Web Agent listens)
- Timeout
- Status Last Modified
- Last Modified
- Last Modified By

Related Topics:

Use Table Views

Export Table Information

IP Subnets View (Inventory)

Tip: See "IP Subnet Form" on page 189 for more details about the IP subnet attributes that appear in this view's column headings.

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

For each IP subnet displayed, you can identify its name, prefix, prefix length (**PL**), 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.

[1]The Web Agent represents a management service running on a device and contains the settings NNMi uses to communicate with the device.

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 **Name** 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 189

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 191

Export Table Information

Chassis View

Tip: See "Chassis Form" on page 193 for more details about the Chassis attributes that appear in this view's column headings.

The **Chassis** view in the Inventory workspace is useful for identifying all of the Chassis hosted on the nodes that are stored in the NNMi database. To view the Chassis per node, use the **Managed By** column to sort the view.

See Use Table Views for more information about sorting, filtering, and hiding attribute columns within a view.

To display the Chassis view:

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

For each Chassis displayed in this view, you can identify the Chassis Status, Administrative State, Operational State, name of the associated node (Managed By), the date and time the Status was last modified, the Chassis Name, model type (the hardware manufacturer's designator), Serial Number, Firmware Version, Hardware version, Software Version, Component Identifier number, time the state was last modified, Parent Chassis (name of the chassis, if any, to which the selected child chassis is attached), Redundant Group, if any, in which the chassis participates, and Description.

To see the incidents related to a Chassis:

1. Double-click the row representing a Chassis. The "Chassis Form" on page 193 displays all details about the selected Chassis.
2. Navigate to the **Incidents** tab to see the incidents associated with the selected Chassis.

Related Topics

Use Table Views

Export Table Information

Cards View

Tip: See "Card Form" on page 211 for more details about the Card attributes that appear in this view's column headings.

The **Card** view in the Inventory workspace is useful for identifying all of the Cards associated with the nodes that are stored in the NNMi database. To view the Cards per node, use the **Managed By** column to sort the view.

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 associated node (Managed By), the date and time the Status was last modififed, the Card Name, model, Type (the hardware manufacturer's designator), Serial Number, Firmware Version, Hardware Version, Software Version, Component Identifier number, Physical Index number, Parent Card (name of the card, if any, in which the selected child card is attached), Redundant Group, if any, in which the card participates, the date and time the State was last modified, 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 211 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 229 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, Type (hardware-type designator), Speed, Configured Duplex Setting, if any, the Card on which the Port resides, the interface to which the Port is associated, and any ifAlias.

Related Topics

Use Table Views

Export Table Information

Node Sensors View

Tip: See "Node Sensor Form" on page 232 for more details about the node sensor attributes that appear in this view's column headings. Node Sensors are displayed in three views: "Node Sensors View" above, "Non-Normal Node Sensors View" on page 393, and "Unmanaged Node Sensors View" on page 585.

The **Unmanaged Node Sensor** view in the **Management Mode** workspace is useful for identifying all of the Node Sensors that are not currently being used.

To display the Node Sensors view:

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

For each Node Sensor displayed in the view, you can identify the Status, Name, Type, Hosted On Node, and Status Last Modified time.

Related Topics:

Use Table Views

Export Table Information

Physical Sensors View

Tip: See "Physical Sensor Form" on page 244 for more details about the node sensor attributes that appear in this view's column headings. Node Sensors are displayed in three views: Physical Sensors View, "Non-Normal Physical Sensors View" on page 394, and "Unmanaged Physical Sensors View" on page 585.

To display the Physical Sensors view:

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

For each Physical Sensor displayed in the view, you can identify the Status, Name, Type, Managed By, Hosted On, and Status Last Modified time.

Note: The NNMi administrator can set Physical Sensor thresholds. For more information, see "Chassis Form: Physical Sensors Tab" on page 204 and "Card Form: Physical Sensors Tab" on page 222.

Related Topics:

Use Table Views

Export Table Information

Layer 2 Connections View (Inventory)

Tip: See "Layer 2 Connection Form" on page 255 for more details about the Layer 2 Connection attributes that appear in this view's column headings.

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

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

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 65 for more details about the node attributes that appear in this view's column headings.

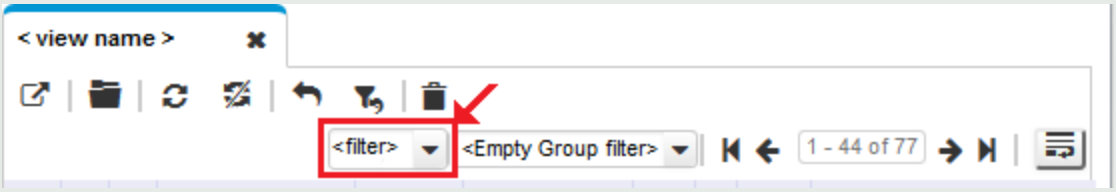
(*NNMi Advanced*) The Global Network Management feature enables multiple NNMi management servers to share the workload in your network environment. See "NNMi's Global Network Management Feature (NNMi Advanced)" on page 29 for more information about this feature.

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:



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 65 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 SNNP agent is enabled, the date indicating the last time the node status was modified, any notes that exist for the node, its system name, (if this is a **virtual machine**[1]) the name of the server this node is hosted on, system contact name, a system description, which NNMi management server is responsible for this node, the Node Management Mode, 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, the date and time the discovery last completed, the creation date, and the date and time the node was last modified.

See "Nodes View (Inventory)" on page 38 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 113 for more details about the interface attributes that appear in this view's column headings.

The **Interfaces (All Attributes)** view in the Inventory workspace 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 date and time the state 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:

[1]A device that utilizes components from multiple physical devices. Depending on the manufacture's implementation, the virtual machine may be static or dynamic.

- 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>]`).

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 160 for more details about the IP address attributes that appear in this view's column headings.

The **Custom IP Addresses** view in the Inventory workspace displays most IP address attribute columns. Sort and filter this IP address view to meet your needs, if the views available in 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, mapped 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, the interface direct management mode, the node 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 (Inventory)

The **MIB Variables** view in the Inventory workspace displays all of the MIB variables currently available in NNMi. These MIB Variables provide pieces of information you can gather from devices in your network upon demand.

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.

   Columns in this view show each MIB variable's numeric OID (Object Identifier), Name, Syntax, source MIB, and textual OID.
3. Double-click any row to display more details about a MIB Variable. See "MIB Variable Form" on page 329.
4. To gather this information from a node, see "Using the MIB Browser" on page 348.

Tip: To quickly filter this view for the information you need, consider the following examples:

`.1.3.6.1` is the base of the Internet MIB structure.

`.1.3.6.1.2.1` is the base of the MIB-2 branch.

`.1.3.6.1.3` is the base of all MIB objects that are for experimental purposes.

`.1.3.6.1.4.1.9` is the base of all MIB objects provided by Cisco.

`.1.3.6.1.4.1.11` is the base of all MIB objects provided by HP.

`.1.3.6.1.5` is the base of the Security MIB branch.

`.1.3.6.1.6` is the base of the SNMPv2c MIB branch.

Related Topics

Use Table Views

Export Table Information

Chassis Redundancy Groups View (Inventory)

Tip: See "Chassis Redundancy Group Form" on page 270 for more details about the attributes that appear in this view's column headings.

The **Chassis Redundancy Groups** view in the Inventory workspace is useful for identifying the names of the groups that provide redundancy protection against chassis failure.

To display the Chassis Redundancy Groups view:

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

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

   See Use Table Views for more information about sorting, filtering, and hiding attribute columns within a view.

To see the incidents related to a Chassis Redundancy Group:

1. Double-click the row representing a Chassis Redundancy Group. The "Chassis Redundancy Group Form" on page 270 displays all details about the selected Chassis Redundancy Group.
2. Navigate to the **Incidents** tab.

   A table displays the list of Incidents associated with the selected Chassis Redundancy Group.

To view the members that belong to this group:

1. Double-click the row representing a Chassis Redundancy Group. The "Chassis Redundancy Group Form" on page 270 displays all details about the selected Chassis Redundancy Group.
2. Navigate to the **Redundant Chassis** tab.

   A table displays the list of Chassis that belong to the selected Chassis Redundancy Group.

Related Topics:

"Chassis Redundancy Groups View (Monitoring)" on page 401

Card Redundancy Groups View (Inventory)

Tip: See "Card Redundancy Group Form" on page 274 for more details about the attributes that appear in this view's column headings.

The **Card Redundancy Groups** view in the Inventory workspace shows the groups of redundant cards that your network administrator configured to provide one-to-one redundancy protection against processor 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 274 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.

   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 a Card Redundancy Group. The "Card Redundancy Group Form" on page 274 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

"Card Redundancy Groups View (Monitoring)" on page 401

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 279 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 279 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 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 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 281 for more details about the Router Redundancy Member attributes that appear in this view's column headings.

To display the Router Redundancy Member view:

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

For each Router Redundancy Member displayed in the view, you can identify the Router Redundancy Member Current State, its Previous State, the Router Redundancy Group Name, the hostname on which the Router Redundancy Member resides, the interface that is being used by the router to participate in the Router Redundancy Group (Redundancy Inteface), 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 Member owns the Virtual IP Address for the Router Redundancy Group (for example, **VRRP**[1] protocol).

Related Topics

Use Table Views

Export Table Information

[1]Virtual Router Redundancy Protocol

Node Groups View (Inventory)

Tip: See "Node Group Form" on page 293 for more details about the Node Group attributes that appear in this view's column headings

The **Node Groups** view in the Inventory workspace is useful for identifying the names of the groups configured by your network administrator.

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 37 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 *HPE 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 293 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, whether its status is calculated, the date and time its status was last modified, and any notes about the node group.

Related Topics

Export Table Information

Interface Groups View (Inventory)

Tip: See "Interface Group Form" on page 302 for more details about the Interface Group attributes that appear in this view's column headings.

The **Interface Groups** view in the Inventory workspace is useful for identifying the names of the groups configured by your network administrator.

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 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 37 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 Groups** 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 113 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, node group, and any notes about the interface group.

Related Topics

Export Table Information

Performance Analysis with Additional Views

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

NNMi presents a new workspace in the NNMi console — the **Performance Analysis** workspace. The Performance Analysis workspace contains two additional views—Node Performance Metrics and Interface Performance Metrics. These views show details of nodes and interfaces on which performance monitoring is enabled.

Within these views, you can see average values of key performance metrics collected from nodes and interfaces on which performance monitoring is enabled. You can launch forms from these views to see detailed status information of each node or interface.

Node Performance Metrics

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

The Node Performance Metrics view is useful in analyzing the performance of nodes on which performance monitoring is configured.

For each node displayed, you can identify the average value of each of the following performance metrics:

- CPU 1Min Utilization (avg)
- Memory Utilization (avg)
- Node Reachability (avg)

- Node Availability (avg)
- ICMP Response Time (msec) (avg)
- Buffer Utilization (avg)
- Disk Utilization (avg)

In addition, the view displays the status (critical, major, warning, minor, or normal) of the following metrics:

- CPU 1Min Utilization (avg)
- Memory Utilization (avg)
- Node Availability (avg)
- Buffer Utilization (avg)
- Disk Utilization (avg)

The "Status Category Defaults" below shows the default range of values represented by each status category. You can configure the range of values represented by each status category (see " Configure Status Categories").

Status Category Defaults

Severity	CPU 1Min Utilization	Memory Utilization (avg)	Node Availability (avg)	Buffer Utilization (avg)	Disk Utilization (avg)
Normal	0 - 25	0 - 25	90 - 100	0 - 25	0 - 25
Minor	25 - 50	25 - 50	75 - 90	25 - 50	25 - 50
Warning	50 - 75	50 - 75	50 - 75	50 - 75	50 - 75
Major	75 - 90	75 - 90	25 - 50	75 - 90	75 - 90
Critical	90 - 100	90 - 100	0 - 25	90 - 100	90 - 100

If no values are retrieved for a metric, the status is shown as Unknown ( ).

If you double-click a node, the Node Form opens. This Node Form is identical to the Node Form that you can open from the Node view in the Inventory workspace.

You can filter the rows in this table view by:

- A predefined Node Group
- Time range; available options are: last hour (default), last 12 hours, last day
- Top contributor counts; available options are: 200 (default), 500, 1000

You can right-click a node and click **Open Dashboard** to launch a dashboard.

Configure Status Categories

To configure the range of values expressed by each status category:

1. Log on to the NNMi management server.
2. Go to the following directory:

   Windows: `%nnmdatadir%\shared\perfSpi\conf`

Linux: `/var/opt/OV/shared/perfSpi/conf`

3. Open the `node-performance-range.properties` file with a text editor.
   The default file contains the following content:

```
cpu1min=0,25,50,75,90,100
memory=0,25,50,75,90,100
bufutil=0,25,50,75,90,100
nodeavail=100,90,75,50,25,0
diskutil=0,25,50,75,90,100
```

   For each metric:
   - Normal indicates the range between the first and second numbers
   - Minor indicates the range between the second and third numbers
   - Warning indicates the range between the third and fourth numbers
   - Major indicates the range between the fourth and fifth numbers
   - Critical indicates the range between the fifth and sixth numbers
4. Make necessary changes to set non-default ranges for each category.
5. Save the file. Changes take effect as soon as you refresh the view.

Interface Performance Metrics

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

The Interface Performance Metrics view is useful in analyzing the performance of Interfaces on which performance monitoring is configured.

For each Interface displayed, you can identify the average value of each of the following performance metrics:

- Availability (avg)
- Utilization In (avg)
- Utilization Out (avg)
- Throughput In (avg)
- Throughput Out (avg)
- Error Rate In (avg)
- Error Rate Out (avg)
- Discard Rate In (avg)
- Discard Rate Out (avg)

- Queue Drops In (avg)
- Queue Drops Out (avg)
- FCS LAN Error rate (avg)
- FCS WLAN Error Rate (avg)

In addition, the view displays the status (critical, major, warning, minor, or normal) of the following metrics:

- Availability (avg)
- Utilization In (avg)
- Utilization Out (avg)

The "Status Category Defaults" below table shows the default range of values represented by each status category.You can configure the range of values represented by each status category (see "Configure Status Categories" below).

Status Category Defaults

Severity	Availability (avg)	Utilization In (avg)	Utilization Out (avg)
Normal	90 - 100	0 - 5	0 - 5
Minor	80 - 90	5 - 15	5 - 35
Warning	70 - 80	15 - 25	35 - 45
Major	60 - 70	25 - 55	45 - 55
Critical	0 - 60	55 - 100	55 - 100

If no values are retrieved for a metric, the status is shown as Unknown ( ).

If you double-click an Interface, the Interface Form opens. This Interface Form is identical to the Interface Form that you can open from the Interface view in the Inventory workspace.

You can filter the rows in this table view by:

- A predefined Interface Group
- Time range; available options are: last hour (default), last 12 hours, last day
- Top contributor counts; available options are: 200 (default), 500, 1000

You can right-click an interface and click **Open Dashboard** to launch a dashboard.

Configure Status Categories

To configure the range of values expressed by each status category:

1. Log on to the NNMi management server.
2. Go to the following directory:

   Windows: `%nnmdatadir%\shared\perfSpi\conf`

   Linux: `/var/opt/OV/shared/perfSpi/conf`
3. Open the `if-performance-range.properties` file with a text editor.

   The default file contains the following content:

```
availability=100,90,80,70,60,0
utilizationin=0,5,15,25,55,100
utilizationout=0,5,35,45,55,100
```

For each metric:

- Normal indicates the range between the first and second numbers
- Minor indicates the range between the second and third numbers
- Warning indicates the range between the third and fourth numbers
- Major indicates the range between the fourth and fifth numbers
- Critical indicates the range between the fifth and sixth numbers

4. Make necessary changes to set non-default ranges for each category.
5. Save the file. Changes take effect as soon as you refresh the view.

MPLS WAN Clouds (RAMS) View (*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*, plus *HPE Route Analytics Management System (RAMS) for MPLS WAN*) 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**[1] 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

[1]An Autonomous System (AS) is a collection of connected Internet Protocol (IP) routing prefixes that present a common, clearly defined Border Gateway Protocol (BPG) routing policy to the Internet by having an officially registered Autonomous System Number (ASN).

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 482for 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 65
- Interface Form 113
- IP Address Form 160
- SNMP Agent Form 168
- Web Agent Form (NNMi Advanced) 181
- IP Subnet Form 189
- VLAN Form 191
- Chassis Form 193
- Card Form 211
- Port Form 229
- Node Sensor Form 232
- Physical Sensor Form 244
- Layer 2 Connection Form 255
- Chassis Redundancy Group Form 270
- Card Redundancy Group Form 274
- Router Redundancy Group Form (NNMi Advanced) 279
- Node Group Form 293
- Interface Group Form 302
- MPLS WAN Cloud (RAMS) Form (NNMi Advanced) 305
- Custom Node Collections Form 307

You can also access:

- "MIB Variable Form" on page 329
- "Router Redundancy Member Form (NNMi Advanced)" on page 281

- "Incident Form" on page 437

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 also right-click any object in a table or map view to access the items available within 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 tool bar.
3. The form displays, containing details of all information related to the object.
4. View or edit the details of the selected object.

From an Analysis Pane, to view all details associated with an object:

1. - **Access the Analysis Pane from a table view:**
     i. Select the workspace of interest (for example, **Inventory**).
     ii. Select the view that contains the object of interest (for example, the **Nodes** view).
     iii. Select the row that contains the object of interest.
     iv. NNMi displays detailed information at the bottom of the view in the Analysis Pane.
   - **Access the Analysis Pane in a map view:**
     i. Select the workspace of interest (for example, **Topology Maps**).
     ii. 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.

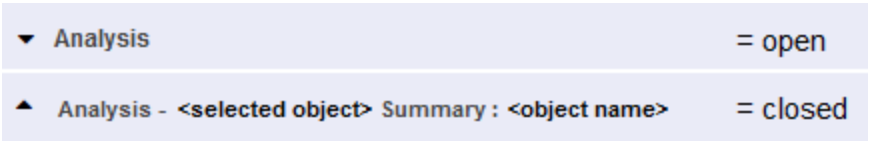
     iii. Click the map object of interest.
     iv. NNMi displays detailed information at the bottom of the view in the Analysis Pane.
   - **Access the Analysis Pane in a form:**
     - Click the form's toolbar Show Analysis icon to display information about the current form's top-level object in the Analysis 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.

2. Open the Analysis Pane if necessary by clicking the expand button in the Analysis Pane banner bar:



   If you change views, NNMi clears the Analysis Pane. The Analysis Pane remains blank unless an object is selected.

   If you select multiple objects, the Analysis Pane displays data about the first selected object.

3. Using the Analysis Pane:
   - To resize, place your mouse cursor over the title bar to display the ↕ symbol and drag to adjust the size.
   - To refresh a subset of information in the Analysis Pane, click any displayed Refresh icon .

     To refresh all data in the Analysis Pane, open the object's form and click Refresh or Save.
   - 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.
   - 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 Sensors of type CPU, Memory, or Buffers, and Physical Sensors of type 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 *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.

     - Each gauge displays the current OID value, using the default refresh rate of 15 seconds.

       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 of the *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.

     - 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.

If a gauge label appears to be a duplicate value, mouse over the label to view the more complete tooltip name that appears.

Tip: If you are an NNMi administrator, to change the gauge title - for example, to the SNMP MIB variable name - see the "Maintaining NNMi" chapter of the *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.)

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 **SNMP Agent**[1], the **Web Agent**[2], 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:

Tip: To see details about the SNMP Agent and Web Agent associated with the node, go to the Managing Agents section in the General tab. Click on the Agent Name in any row to see more details about the status of each agent by opening the SNMP Agent form or Web Agent form.

Basic Attributes

Attribute	Description
Name	The dynamically generated name assigned to this device. The NNMi administrator configures how NNMi populates this attribute through two configuration settings: (1) The **Node Name Resolution** attributes in Discovery Configuration (full or short DNS name, full or short sysName, IP address). (2) The Name *might be* converted to all uppercase or all lowercase (depending on how the NNMi administrator configured settings in the `nms-topology.properties` file). See the

[1]Simple Network Management Protocol (SNMP) is an Internet-standard protocol used to manage devices on IP networks. The SNMP Agent uses this protocol to report information to authorized management programs.
[2]The Web Agent represents a management service running on a device and contains the settings NNMi uses to communicate with the device.

Basic Attributes, continued

Attribute	Description
	"Modifying NNMi Normalization Properties" section of the *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`. This name is used in table views and maps.
Hostname	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). 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. • 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). When the NNMi administrator chooses **Enable SNMP Address Rediscovery** ☑ in the Communication Configuration: ◦ If the SNMP Agent does not respond, NNMi checks for another Management Address to request the Hostname, and the Hostname could change. ◦ If the SNMP Agent associated with the node changes, the Management Address and Hostname could change. When the NNMi administrator disables **Enable SNMP Address Rediscovery** ☐ in the Communication Configuration, when the current management address (SNMP agent) becomes unreachable, NNMi does not check for other potential management addresses. • 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. **Note:** NNMi administrators can use NNMi property file settings to change the way NNMi determines Hostname values: • `nms-topology.properties` 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 *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`. • `nms-disco.properties` 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

Basic Attributes, continued

Attribute	Description
	the "Maintaining NNMi" chapter of the *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.
Management Address	IP address NNMi uses to communicate with this node through SNMP. This is the IP address of the device's SNMP agent. **Tip:** The NNMi administrator can specify an address (Communication Configurations workspace, Specific Node Settings tab), or NNMi can dynamically select one. When NNMi first discovers a node, the *seed address* (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. **Note:** (*NNMi Advanced*) The NNMi administrator specifies whether NNMi prefers IPv4 addresses, IPv6 addresses, or dual-stack (both) when selecting the Management Address. See Configure Default SNMP, Management Address, and ICMP Settings. 1. NNMi ignores the following addresses when determining which Management Address is most appropriate: • Any address of an administratively-down interface. • Any address that is virtual (for example, **VRRP**[1]). • Any IPv4 **Anycast Rendezvous Point IP Address**[2] or IPv6 Anycast address. • Any address in the reserved loopback network range. IPv4 uses 127/24 (`127.*.*.*`) and IPv6 uses `::1`. • Any **IPv6 link-local address**[3]. 2. If the NNMi Administrator chooses **Enable SNMP Address Rediscovery** ☑ in Communication Configuration, NNMi prefers the last-known Management Address (if any). 3. If the Management Address does not respond and the NNMi Administrator specifies

[1]Virtual Router Redundancy Protocol
[2]Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.
[3]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
	Enable SNMP Address Rediscovery in Communication Configuration, NNMi uses the Communication Configuration settings for *Management Address Selection*. The NNMi Administrator chooses the order in which NNMi checks the following: • 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. • Lowest Loopback - If a node supports multiple **loopback address**[1], 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). • Highest Loopback - If a node supports multiple **loopback address**[2], 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. • Interface Matching - The NNMi Administrator chooses which interface MIB variable NNMi queries to detect changes. NNMi can use the following MIB-II attribute values: `ifIndex`, `ifName`, `ifDescr`, `ifAlias`, or a combination of these (`ifName` or `ifDescr`, `ifName` or `ifDescr` or `ifAlias`). NNMi searches current database entries for information about the interface in this order: index, alias, name, and description. If multiple IP addresses are associated with the interface, NNMi starts by querying the lowest IP address and selects the first responding address in ascending order. 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. 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).

[1]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.
[2]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
	Note: The address represents a *static* Network Address Translation (NAT) pair's *external IP address* 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. 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 *SNMP Minimum Security Level* settings). 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. 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 **Enable SNMP Address Rediscovery** ☐ (disabled) or *Preferred Management Address* setting. If this field shows unexpected results: • Use the **Actions** → **Polling** → **Configuration Poll** command to gather the most current information about this node. **Tip:** You can also right-click any object in a table or map view to access the items available within the **Actions** menu. • Check with your NNMi administrator. The NNMi administrator can configure a specific management address for this node in the Communication Configuration settings. **Note:** If the device does not support SNMP, this field is empty.
Status	Overall status for the current node. NNMi follows the ISO standard for status classification. See the "Node Form: Status Tab" on page 93 for more information. Possible values are: No Status Normal Disabled Unknown Warning Minor

Basic Attributes, continued

Attribute	Description
	Major Critical The status of all IP addresses and the SNMP associated with this node contribute to node status. For information about how the current status was determined, see the Conclusions tab. Status reflects the most serious outstanding conclusion. See "Watch Status Colors" on page 406 for more information about possible status values. (*NNMi Advanced*) If a Web Agent is associated and the node is a Virtual Machine, note that the following categories indirectly indicate the current condition of the **hypervisor**[1]: Indicates that the hypervisor is Up Indicates that the hypervisor is Down Indicates a Null value in hypervisor state **Note:** The icons are displayed only in table views.
Power State	(*NNMi Advanced*) NNMi displays this attribute only in Node forms of VMware virtual machines: **Powered On** – Indicates the device is turned on. **Powered Off** – Indicates the device is turned off. **Suspended** – Indicates the device is suspended. The following values indicate NNMi could not gather the required data: **Agent Error** – Indicates an error was returned in response to the query. **No Polling Policy** - No polling policy exists for this monitored attribute. **Not Polled** - 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. **Not Provided** — The device does not support providing information for this monitored attribute. **Unavailable** - The agent responded with a value outside the range of possible values or returned a null value. **Unset** – Currently not used by NNMi.

[1]The virtual machine manager in charge of delegating various aspects from a pool of resources to become virtual devices. The delegations might be static or dynamic, depending on the manufacture's implementation. The type of virtual machines being generated depends on the manufacturer's implementation.

Basic Attributes, continued

Attribute	Description
Node Management Mode	Indicates whether or not NNMi is currently monitoring the node. Possible values are: **Managed** – Indicates the node is managed by NNMi. **Not Managed** – 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. **Out of Service** – Indicates a node is unavailable because it is out of service or participating in a Scheduled Node Outage. NNMi does not update discovery information or monitor these nodes. See the Outage History tab for more details. NNMi administrators and Level 2 Operators can use the drop-down selection list to change the current setting. NNMi uses this setting in a variety of ways. See "How NNMi Assigns the Management Mode to an Object" on page 591. (*NNMi Advanced - Global Network Management feature*) 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.) **Note:** If the NNMi Security configuration permits, you can change this setting using **Actions** → **Management Mode**. To change the Management Mode back to **Managed** for the selected Node object and change the Management Mode back to **Managed** or **Inherited** for all associated interfaces and addresses, use the **Actions** → **Management Mode** → **Managed (Reset All)**.
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. Click the Lookup icon and select Open to display the "Device Profile Form" on page 107 for more information.
Security Group	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. 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. **Note:** This attribute displays after the NNMi administrator defines more than one Security Group.
Hosted On Node	(*NNMi Advanced*) This attribute appears when you are viewing a node form for either: • a partitioned virtual instance of another node

Basic Attributes, continued

Attribute	Description
	• a **virtual machine**[1] (hosted by a **hypervisor**[2]) This attribute is the Name of the node hosting (providing) this virtual 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). Click the Lookup icon and select Show Analysis or Open to display more information about the host node. **Tip:** When the form you are viewing represents a virtual machine (hosted by a hypervisor), this attribute might temporarily not be known. For example: • NNMi might discover the virtual machine before discovering the hypervisor. • The hypervisor owning this virtual machine has recently changed. NNMi has not yet gathered details from the new hypervisor.
Tenant	Tenants enable NNMi administrators to partition a network across multiple customers. A Tenant is the top-level organization to which a Node belongs. 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 Change Tenant Assignment for a Node. Devices that belong to the Default Tenant can have Layer 2 Connections to any device in any Tenant. Devices within any Tenant *other than* Default Tenant can have Layer 2 Connections *only* to devices within the same Tenant or the Default Tenant.
NNMi Management Server	(*NNMi Advanced*) This attribute only appears if the Global Network Management feature is enabled and you are using a Global Manager. See "NNMi's Global Network Management Feature (NNMi Advanced)" on page 29 for more information. 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.

[1]A device that utilizes components from multiple physical devices. Depending on the manufacture's implementation, the virtual machine may be static or dynamic.
[2]The virtual machine manager in charge of delegating various aspects from a pool of resources to become virtual devices. The delegations might be static or dynamic, depending on the manufacture's implementation. The type of virtual machines being generated depends on the manufacturer's implementation.

Discovery Attribute

Attribute	Description
Discovery State	Current discovery status for the node. Possible values are: **Newly Created** – 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. **Discovery Completed** – Indicates that NNMi collected all of the required information about the node. **Rediscovery in Process** – Indicates NNMi is updating information about the node.
Last Completed	Time of the last discovery cycle.

Notes Attribute

Attribute	Description
Notes	(*NNMi Advanced - Global Network Management feature*) 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 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. Type a maximum of 1024 characters. Alpha-numeric, spaces, and special characters (~ ! @ # $ % ^ & * ( ) _+ -) are permitted. **Note:** You can sort your node table views based on this value. Therefore, you might want to include keywords for this attribute value.

Node Form: General Tab

The "Node Form" on page 65 provides details about the selected node.

For information about each tab:

System Properties

Attribute	Description
System Name	The MIB II sysName value returned from the device's SNMP agent. This attribute is set by the device administrator. 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

System Properties, continued

Attribute	Description
	default name by following a set of rules. Click here for details. 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. To view the Device Profile associated with this node, locate the Device Profile attribute 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.

Managing Agents

Attribute	Description

Agent Type	Type of the agent (SNMP or Web).
	Tip:
	• Each physical device configured with an SNMP Agent will have an SNMP Agent.
	• Each **hypervisor**[1] could have two agents:
	  • SNMP Agent gathering **SNMP**[2] data.
	  • Web Agent gathering **SOAP**[3] data from the VMware VSphere® WebService.
	• Each virtual machine provided by the hypervisor has only the Web Agent.

Agent Name	Indicates whether the agent is an SNMP Agent or Web Agent. For Web Agents hosted on VMware hypervisors, the field shows VMware vSphere.

[1]The virtual machine manager in charge of delegating various aspects from a pool of resources to become virtual devices. The delegations might be static or dynamic, depending on the manufacture's implementation. The type of virtual machines being generated depends on the manufacturer's implementation.
[2]Simple Network Management Protocol
[3]Simple Object Access Protocol

Managing Agents, continued

Attribute	Description
	For SNMP Agents, the field shows the combination of the SNMP version used by the agent (for example, SNMPv2c) and the IP address of the agent. To see more details about an **SNMP Agent**[1] or **Web Agent**[2], click the agent name to open the SNMP Agent form or Web Agent form.
Hosted On	The FQDN or IP address of the system that hosts the agent.
Agent Status	The status of the node that hosts the agent.
Agent State	Indicates whether the agent assigned to this node is available and how NNMi is interacting with this agent. Possible values are: For the SNMP Agent: **Normal** – Indicates that the agent responds to requests requiring authentication and login. **Not Responding** – Indicates that the SNMP agent does not respond to requests requiring authentication and login. **Not Polled** – 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. **No Polling Policy** – Indicates that this SNMP Agent's address is being polled, but no polling policy exists in any Monitoring Configuration settings for this monitored attribute. **Unset** – Currently not used by NNMi. For the Web Agent: **Normal** – Indicates that the agent responds to requests requiring authentication and login. **Not Responding** – Indicates that the Web Agent does not respond to requests requiring authentication and login. **Not Polled** – Indicates that this Web Agent 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 Web Agent might or might not have an associated polling policy. **No Polling Policy**– Indicates that this Web Agent is being polled, but no polling policy

[1]Simple Network Management Protocol (SNMP) is an Internet-standard protocol used to manage devices on IP networks. The SNMP Agent uses this protocol to report information to authorized management programs.
[2]The Web Agent represents a management service running on a device and contains the settings NNMi uses to communicate with the device.

Managing Agents, continued

Attribute	Description
	exists. **Unset** – Currently not used by NNMi. State is determined by the State Poller Service. The current state contributes towards the status calculation for the node. See the Node Form: Status tab for more information.
SNMP Agent Enabled	Indicates whether the agent is set up to communicate with NNMi.

Node Form: IP Addresses Tab

The "Node Form" on page 65 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	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. Double-click the row representing an IP address. The "IP Address Form" on page 160 displays all details about the selected IP address.

Node Form: Interfaces Tab

The "Node Form" on page 65 provides details about the selected node.

For information about each tab:

Interfaces Table

Attribute	Description
Interfaces	Table view of all of the interfaces associated with the current node. If the interface is physical, 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. If NNMi is also managing a virtual environment, use this table to also view the details about any interface that represents a virtual switch. These interfaces will have either a blank or 0 bps IfSpeed value. Double-click the row representing an interface. The "Interface Form" on page 113 displays all details about the selected interface.

Node Form: Virtual Switches Tab

(*NNMi Advanced*) The "Node Form" on page 65 provides details about the selected **hypervisor**[1] node.

Note the following:

- Use the **Virtual Switches** tab to view details of the virtual switch (also known as **virtual bridge**) configured on the selected node.
- For devices that implement virtual switches (or bridges) as a network interface, these interfaces are identified using the **Virtual Bridge** capability.
- When you select a virtual switch from the table, the Analysis Pane includes tabs for the associated **Uplinks** and **Virtual Ports**.

For information about each tab:

Virtual Switches Table

Attribute	Description
Interfaces	Table view of all of the interfaces representing a virtual switch that is configured on the selected hypervisor. Double-click the row representing a virtual switch. The "Virtual Switch's Interface Form (NNMi Advanced)" on page 155 displays all details about the selected interface that represents a virtual switch.

Node Form: Chassis Tab

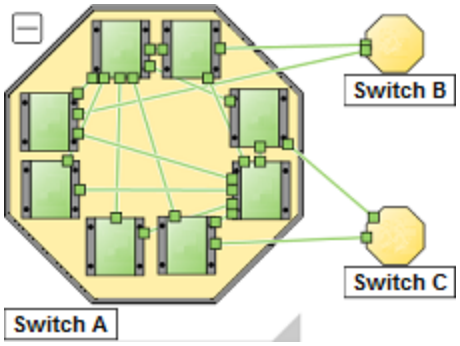
The "Node Form" on page 65 provides details about the selected node.

When more than one Chassis is listed in this tab, the map icon changes to a stacked image:

Node	Switch	Switch-Router

Click to display the entire group of Chassis. If your NNMi role allows, click the Save Map toolbar button to keep the Chassis visible when you return to that map in the future. For example:

[1]The virtual machine manager in charge of delegating various aspects from a pool of resources to become virtual devices. The delegations might be static or dynamic, depending on the manufacture's implementation. The type of virtual machines being generated depends on the manufacturer's implementation.



For information about each tab:

Tip: If the current node reports a list of Hosted Nodes, this is the group of chassis used by this node and all its hosted nodes.

Chassis Table

Attribute	Description
Chassis	Table view of all of the Chassis associated with the current Node. Double-click the row representing a Chassis. The "Chassis Form" on page 193 displays all details about the selected Chassis.

Node Form: Cards Tab

The "Node Form" on page 65 provides details about the selected node.

For information about each tab:

Tip: If the current node reports a list of Hosted Nodes, this is the group of cards used by this node and all its hosted nodes.

Cards Table

Attribute	Description
Cards	Table view of all of the cards associated with the current node. Double-click the row representing a Card. The "Card Form" on page 211 displays all details about the selected Card.

Node Form: Ports Tab

The "Node Form" on page 65 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 access information about each port associated with the selected node. Double-click the row representing a port. The "Port Form" on page 229 displays all details about the selected port.

Node Form: VLAN Ports Tab

Tip: The "Node Form" on page 65 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	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. Double-click the row representing a VLAN port. The "VLAN Port Form" below displays all details about the selected VLAN port.

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	VLAN connections are determined by a common VLAN Id. The *name* assigned to that VLAN can be designated by each participating Node/Interface's configuration settings for that VLAN Id. Local VLAN Name = the VLAN name assigned by the configuration settings on the currently selected Node/Interface. **Tip:** If you see an attribute named *Global VLAN name* = NNMi uses the lowest sort-order name from all available names designated by member Nodes assigned to that VLAN.
VLAN Id	The identification value for the current VLAN. This value is taken directly from the MIB file provided by the Vendor.

Basic Attributes, continued

Attribute	Description
	Click the Lookup icon and select Show Analysis or Open to display more information about the VLAN.
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 65

"Interface Form" on page 113

"VLAN Form" on page 191

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

The "Node Form" on page 65 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 279 displays all details about the selected Router Redundancy Group.

Node Form: Capabilities Tab

The "Node Form" on page 65 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**[1] group.

[1]Hot Standby Router Protocol

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 Node. Use this table to access information about each Capability. Double-click the row representing a Node Capability to open the "Node Capability Form" on page 83 and view more information. For more information, see "Node Capabilities Provided by NNMi" below.

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 Capability Attribute Values that are assigned to Nodes (*)

  These Node Capabilities assist in determining Node Sensor metrics. See "Node Form: Node Sensors Tab" on page 84 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 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*> = chassis, card, ipaddr (address), iface (interface), lag (**Link Aggregation**[1] or **Split Link Aggregation**[2] interface), node, rrp (Router Redundancy), or metric (Node Sensor or Physical Sensor).

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

<*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 107).
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 107).

Node Sensor Capability Attribute Values that are assigned to Nodes

Unique Key	Capability	Description
com.hp.nnm.capability.rams.node.ramsmplswancen ode	MPLS WAN CE No de	(*NNMi Advanced*, plus *HPE Route Analytics Management System (RAMS) for MPLS WAN*) The node supports HPE Router Analytics Management System (RAMS) and MPLS WAN. If you are an NNMi administrator, see HPE RAMS MPLS WAN Configurati on (NNMi Advanced) for information about configuring RAMS.

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	(*NNMi Advanced*) The node is a member of a Virtual Router Redundancy Protocol (VRRP)group.

(*NNMi Advanced*) VMware ESX Host and Virtual Machine Capability Attribute Values

Unique Key	Capability	Description
com.hp.nnm.capability.node.VM	Virtual Machine	(*NNMi Advanced*) The node is a **virtual machine**[1] being hosted on a **hypervisor**[2]. 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	(*NNMi Advanced*) A VMware 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**[3] group.

[1]A device that utilizes components from multiple physical devices. Depending on the manufacture's implementation, the virtual machine may be static or dynamic.
[2]The virtual machine manager in charge of delegating various aspects from a pool of resources to become virtual devices. The delegations might be static or dynamic, depending on the manufacture's implementation. The type of virtual machines being generated depends on the manufacturer's implementation.
[3]Hot Standby Router Protocol

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.

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 80 shows a list of all available Capabilities for that node. For more information, see "Node Capabilities Provided by NNMi" on page 81.
Unique Key	Used as a unique identifier for the Capability. Any capability provided by NNMi begins with the prefix `com.hp.nnm.capability`. For more information, see "Node Capabilities Provided by NNMi" on page 81.

Node Form: Node Groups Tab

The "Node Form" on page 65 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 "Node Group Form" on page 293 displays all details about the selected Node Group. **Caution:** If you click Delete from this table view, the Node Group is deleted.

Node Form: Node Sensors Tab

The "Node Form" on page 65 provides details about the selected node.

For information about each tab:

The Node Form: Node Sensors tab displays information about node fault and performance metrics:

- 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 HPE Network Node Manager iSPI Performance for Metrics

Software is installed and configured within your environment, the NNMi administrator can configure threshold for the following performance metrics (click here for more information):

- 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.

Tip: See "Node Sensor Form" on page 232 for more details about the node sensor attributes that appear in this view's column headings. Node Sensors are displayed in three views: "Node Sensors View" on page 47, "Non-Normal Node Sensors View" on page 393, and "Unmanaged Node Sensors View" on page 585.

Node Sensors Table

Attribute	Description
Node	Table view of the fault and performance metrics associated with the current node. You can use

Node Sensors Table, continued

Attribute	Description
Sensors	this table to determine the Status, Name, and Type for each Node Sensor metric associated with the selected node. Double-click the row representing a Node Sensor. The "Node Sensor Form" on page 232 displays all details about the selected Node Sensor. **Note:** The NNMi administrator can set Node Sensor thresholds. For more information, see "Node Form: Node Sensors Tab" on page 84, "Chassis Form: Node Sensors Tab" on page 205, and "Card Form: Node Sensors Tab" on page 223.

Node Form: Hosted Nodes Tab

(*NNMi Advanced*) The Node Form: Hosted Nodes tab appears if the Node is hosting other Nodes. For example, a virtual device.

For information about each tab:

The Nodes listed on this tab will have a Hosted On Node attribute showing the Hostname of the hosting Node.

Tip: These nodes share the group of Chassis and Cards managed by the hosting node.

Hosted Nodes Table

Attribute	Description
Status	See the Status information in "Node Form" on page 65.
Device Category	The NNMi administrator specifies this attribute value. See Configure Device Category Icons.
Name	See the Name information in "Node Form" on page 65.
Hostname	See the Hostname information in "Node Form" on page 65.
Management Address	See the Management Address information in "Node Form" on page 65.
System Location	See the System Location information in "Node Form: General Tab" on page 73.
Device Profile	See the Device Profile information in "Node Form" on page 65.
SNMP Agent Enabled	See the SNMP Agent Enabled information in "Node Form" on page 65.
Status Last Modified	See the Status Last Modified information in "Node Form: Status Tab" on page 93.
Notes	See the Notes information in "Node Form" on page 65.

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. See "Custom Node Attribute Samples" on the next page.

The Node Form: Custom Attributes tab displays a table view of any Custom Attributes that have been added to the selected node.

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 can be replicated from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager configure which Regional Custom Attributes they want (Global Manager: Configure Custom Attribute Replication). NNMi administrators can also configure Custom Attribute values that are unique to the Global Manager's environment (Customize Object Attributes).

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 Node forms. Limit 50 of any combination of keyboard entries including spaces.
Value	Value assigned to the Custom Attribute for the selected node. Limit 2,000 of any combination of keyboard entries including spaces. For more information, see "Custom Node Attributes Form" below.

The Custom Attributes tab for a virtual machine or a hypervisor node shows three following default attributes: PartitionHost, PartitionID, and PartitionName.

Default Custom Attributes

Attribute	Description
PartitionHost	• *For a virtual machine:* UUID of the hypervisor that hosts the virtual machine • *For a hypervisor:* UUID of the hypervisor
PartitionID	UUID of the node
PartitionName	Hostname of the node

Custom Node Attributes Form

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

Samples" on the next page.

The required settings for these attributes are described in the table below.

(*NNMi Advanced - Global Network Management feature*) Custom Attribute values can be replicated from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager configure which Regional Custom Attributes they want (Global Manager: Configure Custom Attribute Replication). NNMi administrators can also configure Custom Attribute values that are unique to the Global Manager's environment (Customize Object Attributes).

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. Limit 50 of any combination of keyboard entries including spaces.
Value	Value assigned to the Custom Attribute for the selected node. Limit 2,000 of any combination of keyboard entries including spaces. For more information, see "Node Form: Custom Attributes Tab" on the previous page.

Custom Node Attribute Samples

Custom Attributes provide additional information about an object instance:

- To make inventory tasks easier:

  For example, your NNMi administrator might have added the following:

  - **Name**: `Serial Number`
  - **Value**: `UHF536697J3`

- To customize a device icon on the NNMi maps.

  For example, your NNMi administrator can use Custom Attributes to customize the Device Profile icon for one or more nodes (Customize Device Profile Icons):

  - **Name**: `NNM_ICON`
  - **Value** = `<filename of the icon for the selected nodes>`

  To view the list of available device profile icons, see View the Device Profile Icons Available.

- External applications that have been integrated with NNMi can associate custom information with the Interface.

  For example, when *HPE Network Node Manager iSPI Performance for Metrics Software* is installed, your NNMi administrator can provide additional Node or Interface information in NNM iSPI Performance for Metrics reports:

- **Name** = `NPS Annotation`
- **Value** = *<text to appear in the reports>*.

See the help topic: Annotate NNM iSPI Performance for Metrics Reports Reports.

- To make configuring a Scheduled Outage easier by making the Node's Time Zone visible in the Scheduled Node Outage dialog:

  For example, your NNMi administrator might have added the following:

  - **Name**: com.hp.nnm.topo.TZ
  - **Value**: *<any Java Time Zone designator>*

    The list of valid Java Time Zones changes over time. Open the Scheduled Node Outage dialog and click the Time Zone drop-down to display the list of valid choices at this time. See "Scheduling Outages for Nodes or Node Groups" on page 322.

    To check NNMi's current Java Time Zone version number, on the server where NNMi is installed, use the following command line tool (see About Environment Variables for more information)

    Windows:

    `%NnmInstallDir%\jdk\hpsw\bin\java -version`

    Linux:

    `$NnmInstallDir/jdk/hpsw/bin/java -version`

(*NNMi Advanced - Global Network Management feature*) Custom Attribute values can be replicated from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager configure which Regional Custom Attributes they want (Global Manager: Configure Custom Attribute Replication). NNMi administrators can also configure Custom Attribute values that are unique to the Global Manager's environment (Customize Object Attributes).

Related Topics:

"Node Form: Custom Attributes Tab" on page 87.

"Custom Node Attributes Form" on page 87

Node Form: Custom Polled Instances Tab

Tip: The "Custom Polled Instance Form" on page 312 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	The State of the Custom Polled Instance as determined by any Thresholds (High State / Low State 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. Possible State values for a *Polled Instance* (Threshold = High State/Low State; or Comparison Map = State Mapping) are: Normal Warning Minor Major Critical **Note:** The most severe Threshold High State or Low State value or Comparison Map *State Mapping* value returned from the Polled Instances for a Custom Node Collection becomes the Custom Node Collection Status.
MIB Variable	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. Click the Lookup icon and select Show Analysis or Open to display more information about the MIB Variable. See "MIB Variable Form" on page 329 for more information about the MIB Variable attribute.
MIB Instance	This attribute contains the multiple filtered instances for the MIB Expression. Each instance value identifies a row in the MIB table. **Note:** 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	The value from the MIB Expression that caused the State to change.

Basics Attributes, continued

Attribute	Description
Change Value	**Note:** A value of **null** 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

The "Node Form" on page 65 provides details about the selected node.

When you access the Node Form: Diagnostics Tab, you can view the history of all the NNM iSPI NET 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**.

Tip: You can also right-click any object in a table or map view to access the items available within 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	Requires HPE Network Node Manager iSPI Network Engineering Toolset Software (NNM iSPI NET) and requires installation of a Diagnostic Server -- click here for more information. 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. Double-click the row representing a Node Diagnostic Result . The "Node Diagnostic Results Form (Flow Run Result)" below displays all details about the selected Node Diagnostic Result.

Node Diagnostic Results Form (Flow Run Result)

Requires HPE Network Node Manager iSPI Network Engineering Toolset Software (NNM iSPI NET) and

requires installation of a Diagnostic Server -- click here for more information.

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

Tip: You can also right-click any object in a table or map view to access the items available within 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" 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: • The Diagnostic is in the queue, but is not yet running • The Diagnostic has been submitted and is not finished running • The Diagnostic has finished running • An error condition prevented the Diagnostic from being submitted • 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. **Tip:** Example error conditions include the following: • The number of Diagnostics in the queue might prevent NNMI from submitting the Diagnostic. • A configuration error, such as an incorrect user name or password, might prevent NNMi from accessing the required Operations Orchestration server. Contact your NNMi administrator for Diagnostic log file information.
Report	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.

Diagnostics Table, continued

Attribute	Description
Lifecycle State	Incident Lifecycle State of the target Incident. If the incident's Lifecycle State matches the value specified here, the Diagnostic runs. 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).
Last Update Time	Date and time NNM iSPI NET last updated this instance of the Diagnostics report. NNM iSPI NET uses the locale of the client and the date and time from the NNMi management server.

Node Form: Incidents Tab

Tip: See "Incident Form" on page 437 for more details about the incident attributes that appear in the incident table view's column headings.

The "Node Form" on page 65 provides details about the selected node.

For information about each tab:

Incidents Table

Description
Table view of the incidents associated with the selected node. These incidents are sorted by creation time so that you can view the incidents in chronological order. Use this view to determine which incidents are still open for the selected node. Double-click the row representing an incident. The "Incident Form" on page 437 displays all details about the selected incident.

Node Form: Status Tab

The "Node Form" on page 65 provides details about the selected 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

Overall Status, continued

Attribute	Description
	Normal Disabled Unknown Warning Minor Major Critical 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 "Node Form: Conclusions Tab" on the next page. Status reflects the most serious outstanding conclusion. See "Watch Status Colors" on page 406 for more information about possible status values. 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 About Custom Poller for more information. The effect of a Custom Node Collection's Status on the topology node's Status is determined as follows: • If at least one Custom Collection Node's Status is Critical, the topology node Conclusion Status is Critical. • If at least one Custom Collection Node's Status is Major, but none are Critical, the topology node Conclusion Status is Major. • If at least one Custom Collection Node's Status is Minor, but none are Critical or Major, the topology node Conclusion Status is Minor. • At least one Custom Collection Node's Status is Warning, but none are Critical, Major, or Minor, the topology node Conclusion Status is Warning. • If the Status of all Custom Collection Nodes are Normal, the topology node Conclusion Status is Normal. **Note:** The icons are displayed only in table views.
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 status so that you can better determine any patterns in node behavior and activity. Double-click the row representing a Status History. The Status History form displays all details about the selected Status.

Node Form: Conclusions Tab

The "Node Form" on page 65 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	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. Each Conclusion listed is still outstanding and applies to the current overall Status. This view is useful for obtaining a quick summary of the Status and problem description for the current node that led up to the node's most current Status. The Status value is correlated based on the most critical Conclusions. Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion. The following table describes the possible Conclusions that might appear for a node object. **Note:** A **Y** in the **Incident?** column indicates that the Conclusion results in an incident. **Critical Status Conclusions** **Conclusion** / **Description** / **Status** / **Incident?** CustomPollingOnNodeCritical / At least one Custom Polled Instance associated with the physical node has a Status of Critical. / Critical / N NodeDown / The NNMi Causal Engine has / Critical / Y

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	determined the node is down based on the following analysis: • 100% of the addresses assigned to this node are unreachable • NNMi is communicating with at least two of the neighboring devices.		
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

Major Status Conclusions

Conclusion	Description	Status	Incident?
BadPowerSupplyOnHostedNode	At least one of the power supply's monitored attributes on the hosting node (Managed By) or a Hosted Node is outside of the threshold range set on the device.	Major	N
BadTemperatureOnHostedNode	At least one of the monitored attributes for a temperature sensor on the hosting node (Managed By) or a Hosted Node is outside of the threshold range set on the device.	Major	N
BadFanOnHostedNode	At least one of the monitored attributes for a fan on the hosting node (Managed By) or a Hosted Node is outside of the threshold range set on the	Major	N

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	device.		
BadVoltageOnHostedNode	At least one of the monitored attributes for a voltage sensor on the hosting node (Managed By) or a Hosted Node is outside of the threshold range set on the device.	Major	N
BadBackplaneOnHostedNode	At least one of the monitored attributes for the backplane on the hosting node (Managed By) or a Hosted Node is outside of the threshold range set on the device.	Major	N
CardBadBackplaneOnHostedNode	At least one of the monitored attributes for a backplane on the card is outside of the threshold range set on the device.	Major	N
CardBadFanOnHostedNode	At least one of the monitored attributes for a fan on the card is outside of the threshold range set on the device.	Major	N
CardBadPowerSupplyOnHostedNode	At least one of the power supply's monitored attributes on the hosting node is outside of the threshold range set on the device.	Major	N
CardBadTemperatureOnHostedNode	At least one of the monitored attributes for a temperatuere sensor on the card is outside of the threshold range set on the device.	Major	N
CardBadVoltageOnHostedNode	At least one of the	Major	N

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	monitored attributes for a voltage sensor on the card is outside of the threshold range set on the device.		
ChassisMajorInNode	At least one chassis is major in the node.	Major	N
CustomPollingOnNodeMajor	At least one Custom Polled Instance associated with the physical node has a Status of Major.	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

Minor Status Conclusions

Conclusion	Description	Status	Incident?
AllUnresponsiveAddressesInNode	None of the addresses associated with the selected node respond to ICMP ping.	Minor	N
CardDownOnHostedNode	The Operational State of a Card on a Hosted Node is Down.	Minor	N

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	Note: CardDown only propagates to a Hosted Node when a port hosted on that card is used by an interface associated with the node.		
ChassisDownOnHostedNode	The Operational State of a Chassis on a Hosted Node is Down.	Minor	N
CustomPollingOnNodeMinor	At least one Custom Polled Instance associated with the physical node has a Status of Minor.	Minor	N
ChassisDownInNode	The Operational	Minor	N

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	State of a Chassis is Down.		
InterfacesDownInNode	At least one interface contained in the node has an Operational State of Down.	Minor	N
OneOrMoreCardsDownOnHostedNode	At least one card in a Hosted Node has an Operational State of Down. **Note:** CardDown only propagates to a Hosted Node when a port hosted on that card is used by an interface associated with the node.	Minor	N
SNMPAgentPingUnresponsiveInNode	The	Minor	N

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	management address on the node is not responding to ICMP.		
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**[1] associated with this node is not responding to SNMP requests.	Minor	N
UnresponsiveWebAgentInNode	The **Web Agent**[2] associated with this node is not responding	Minor	N

[1]Simple Network Management Protocol (SNMP) is an Internet-standard protocol used to manage devices on IP networks. The SNMP Agent uses this protocol to report information to authorized management programs.
[2]The Web Agent represents a management service running on a device and contains the settings NNMi uses to communicate with the device.

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	to requests.		
StackMinorInNode	A Chassis Redundancy Group contained in the Node has a Status of **Minor**.	Minor	N

Warning Status Conclusions

Conclusion	Description	Status	Incident?
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
ChassisWarningInNode	One card in a chassis has a status of CardDown, but not all cards are down.	Warning	N
ChassisDegradedInNode	More than one card in a chassis has a status of CardDown. Perhaps all cards have a status of CardDown.	Warning	N
StackDegradedInNode	NNMi has detected that a Chassis Redundancy Group contained in the Node is degraded. See "Stack Degraded (NNMi Advanced)" on page 522 for more information.	Warning	N

Disabled Status Conclusions (NNMi Advanced)

Conclusion	Description	Status	Incident?
NodePoweredDown	The Power State of the virtual machine is set to **Powered Off**.	Disabled	Y

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	For example: The virtual machine is turned off.		
NodePaused	The Power State of the virtual machine is set to **Suspended**. For example: The virtual machine is paused.	Disabled	Y

Unknown Status Conclusions

Conclusion	Description	Status	Incident?
NodeUnmanageable	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”. **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.	Unknown	N

Normal Status Conclusions

Conclusion	Description	Status	Incident?
AllInterfacesWithinThresholdBoundariesInNode	All of the interfaces within the selected node are within the allowable threshold range configured by the administrator.	Normal	N
AllResponsiveAddressesInNode	All of the addresses associated with the selected	Normal	N

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	node respond to ICMP ping.		
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 sensors are functioning properly.	Normal	N
ResponsiveAgentInNode	The node's **SNMP Agent**[1] is responding.	Normal	N
ResponsiveWebAgentInNode	The node's **Web Agent**[2] is responding.	Normal	N

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:

- SNMPAgentResponding

[1]Simple Network Management Protocol (SNMP) is an Internet-standard protocol used to manage devices on IP networks. The SNMP Agent uses this protocol to report information to authorized management programs.
[2]The Web Agent represents a management service running on a device and contains the settings NNMi uses to communicate with the device.

Outstanding Status Conclusion Values, continued

Attribute	Description
	• AllResponsiveAddressesInNode • InterfacesUpInNode • CardsUpInNode • CrgNormalInNode

Node Form: Scheduled Outage Tab

The "Node Form" on page 65 provides details about the selected node.

This tab provides a record of all the Node's past, present, and future Scheduled Node Outages. See the "Node Form: Outage History Tab" below for more details.

See also "Scheduling Outages for Nodes or Node Groups" on page 322 and "Scheduled Node Outages View" on page 586.

See "Understand the Effects of Setting the Management Mode to Not Managed or Out of Service" on page 589.

For information about each tab:

Scheduled Outage Table

Attribute	Description
Name	The name assigned to this scheduled outage instance.
Outage Start Time	The date and time that this Scheduled Outage is configured to start.
Outage End Time	The date and time that this Scheduled Outage is configured to end.
Duration	The length of time that the Scheduled Outage is configured to last.

Node Form: Outage History Tab

The "Node Form" on page 65 provides details about the selected node.

This tab provides a record of all this Node's past, present, and future outages (including Scheduled Node Outages).

For information about each tab:

Outage History Table

Attribute	Description
Timestamp	The date and time at which the Management Mode changed for this Node.
Management Mode	The name of the Management Mode change associated with this history instance.
Scheduled Outage	One of the following:

Outage History Table, continued

Attribute	Description
Name	• The name assigned to the Scheduled Outage whose start or stop history is being recorded here. • For all other Management Mode changes, this value is empty (blank).
Modified By	The NNMi User Name of the person who initiated the Node State change. **Note:** If caused by a Scheduled Node Outage, the value is `system`.

Node Form: Registration Tab

The "Node Form" on page 65 provides details about the selected node.

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. **Note:** This value does not change when a node is rediscovered. This is because the Node object is modified, but not created.
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. Note the following: • 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. • 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.

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 65 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 `sysObjectID` number issued for this device type. These numbers are unique across all vendors.
Description	The description, based on information from the MIB-II `sysDescr` string provided by the vendor. Maximum length 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 111 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 111 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 About Map Symbols for more information about the possible values. Click the Lookup icon to access the "Device Category Form" on page 112 for more details.
OUI	Organizationally unique identifier. The first three octets of the MAC address for the device that identify the device's vendor.
Author	Indicates who created or last modified the device profile.

Basic Attributes , continued

Attribute	Description
	Caution: If the Author attribute value is **HP Network Node Manager**, any changes are at risk of being overwritten in the future. • Click **Lookup** and select **Show Analysis** to display details about the currently selected Author. • Click **Quick Find** to access the list of existing Author values. • Click * **New** to create an Author value.

Advanced Settings Tab

Attribute	Description
Use of SNMP SysName for Node Name Resolution	
Never Use sysName	If enabled, Spiral Discovery does not use a MIB-II `sysName` value for the Name attribute for discovered Nodes of this type. If `sysName` is part of the current node Name strategy, NNMi uses the next designated node Name choice in the strategy established by your NNMi administrator. If disabled, MIB-II **sysName** can potentially be used as the Name attribute value for nodes of this type.
Do not Use sysName Starting With	The vendor's default `sysName` text string, from MIB-II `sysName`. If the SNMP agent responds to a sysName request with a value that matches or starts with the entry in this field (case-sensitive), Spiral Discovery ignores the sysName and considers sysName to be unset. As a result, NNMi instead tries to find a DNS name or IP address for this node (according to the strategy established by your NNMi administrator). For example, when an SNMP agent responds with a default `sysName`, NNMi's maps might display multiple icons with the same name (one for every device of that type in your environment that responded to an SNMP query with the default sysName). Usually, the device administrator changes the default sysName value to something more meaningful, so this problem is avoided.
Device Behaviors	
Force Device	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 80). Note the following: • The Force Device attribute does not affect default membership for the Node Groups provided by NNMi. For example, the **Force to router** 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.

Advanced Settings Tab , continued

<table>
<tr><th>Attribute</th><th>Description</th></tr>
<tr><td></td><td>
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.
The following table describes the possible Force Device settings and subsequent behavior:
Force Device Settings and Behavior
<table>
<tr><th>Setting</th><th>Behavior</th></tr>
<tr><td>Do not force</td><td>Ignores the Force Device setting.</td></tr>
<tr><td>Force to router</td><td>Adds the IP Forwarding (Layer 3) Capability to the Node
Displays the device in Layer 3 Neighbor View maps
Checks the Router Redundancy Protocol configuration for information about the Node</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>Removes either of the following Capabilities if they are configured on the Node:
IP Forwarding (Layer 3)
LAN Switching (Layer 2)
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.</td></tr>
<tr><td>Force to switch and router</td><td>Adds the IP Forwarding (Layer 3) Capability to the Node
Adds the LAN Switching (Layer 2) Capability to the Node
Displays the Node in Layer 3 Neighbor View maps
Checks the Router Redundancy Protocol configuration for information about the Node</td></tr>
</table>
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:
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 accurate due to a firmware defect on the device.
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.
The device serves as a virtual router, but should not be managed as a router.
</td></tr>
</table>

Advanced Settings Tab , continued

Attribute	Description
	Setting the Force Device attribute to **Force to end node** 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).
Interface Reindexing Type	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: `ifIndex`, `ifName`, `ifDescr`, `ifAlias`, or a combination of these (`ifName` or `ifDescr`, `ifName` or `ifDescr` or `ifAlias`). See the General Interface Attributes (SNMP Values) in "Interface Form: General Tab" on page 118 for information about these four MIB-II attributes that are available to use for this setting. If you are an Administrator, see Detect Interface Changes for more information.
Prefer LLDP	A network device's interfaces can be configured with proprietary Layer 2 *discovery protocols*, instead of or in addition to the industry standard LLDP (see the list of Topology Source protocols in Layer 2 Connection Form). 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. **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. If NNMi discovers more than one IEEE 802 Layer 2 protocol being used by a particular device's interface, the Device Profile's setting controls NNMi's protocol preference: ☑ **Prefer LLDP** = Enabled: NNMi gives priority to the LLDP data. ☐ **Prefer LLDP** = Disabled: NNMi gives priority to the vendor-specific IEEE 802 Layer 2 protocol data. **Tip:** 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 Troubleshooting Layer 2 Connections.

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 107.

Device Family Definition

Attribute	Description
Label	Device family name. For example, Cisco Catalyst 6500 Series Switches or HP AdvanceStack Routers. 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: `com.<your_company_name>.nnm.device_profile.family.<family_label>` Maximum length is 80 characters. Alpha-numeric characters and periods are permitted. Spaces are not permitted.
Management URL	*Optional*. 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.
Icon	Displays the icon that is associated with the Device Family. If you are an NNMi administrator, you can customize the icon. See Customize Device Profile Icons for more information.

Device Vendor Form

The Device Vendor attribute value indicates the name of the manufacturer of this device type; for example, HPE 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 107.

Device Vendor Definition

Attribute	Description
Label	Vendor name.

Device Vendor Definition , continued

Attribute	Description
	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: `com.<your_company_name>.nnm.device_profile.vendor.<vendor_label>` 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 Customize Device Profile Icons 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 107.

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: `com.<your_company_name>.nnm.device_profile.category.<category_label>` Maximum length is 80 characters. Alpha-numeric characters and periods are permitted. Spaces

Device Category Definition , continued

Attribute	Description
	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 Customize Device Profile Icons for more information.

Interface Form

Click the link to the object type you selected prior to opening the Interface form:

- interface — might be a physical or virtual interface

  For example, the interface might be a virtual port or an uplink provided by a **hypervisor**[1].

- virtual switch

Interface Form

The Interface form provides details about the physical or virtual 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.

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,

[1]The virtual machine manager in charge of delegating various aspects from a pool of resources to become virtual devices. The delegations might be static or dynamic, depending on the manufacture's implementation. The type of virtual machines being generated depends on the manufacturer's implementation.

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 `ifName` value. Second choice is the `ifAlias` value. Third choice is a combination of the `ifType[ifIndex]` value (for example, `ethernetCsmacd[17]`).
Status	Overall status for the current interface. NNMi follows the ISO standard for status classification. See the "Interface Form: Status Tab" on page 140 for more information. Possible values are: No Status Normal Disabled Unknown Warning Minor Major Critical

Basic Attributes, continued

Attribute	Description
	Interface status is derived from SNMP polling results for ifAdminStatus and IfOperStatus, as well as from any conclusions. Status reflects the most serious outstanding conclusion. See the "Interface Form: Conclusions Tab" on page 141 for information about how the current status was determined. See "Watch Status Colors" on page 406 for more information about possible status values. **Note:** The icons are displayed only in table views.
Management Mode	The *calculated* Management Mode for the interface according to the Management Mode Hierarchy. This value reflects the current management mode of this interface's parent object (the Hosted On Node). See "How NNMi Assigns the Management Mode to an Object" on page 591. (*NNMi Advanced - Global Network Management feature*) 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. **Note:** If the NNMi Security configuration permits, you can change this setting using **Actions** → **Management Mode**. **Tip:** You can also right-click any object in a table or map view to access the items available within the **Actions** menu.
Direct Management Mode	Indicates whether or not NNMi is currently monitoring the interface. Possible values are: **Inherited** – Used to indicate that the interface should inherit the Management Mode from this interface's parent object (the Hosted On Node). **Not Managed** – 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. **Out of Service** – Used to indicate an interface is unavailable because it is out of service or participating in a Scheduled Node Outage. NNMi does not discover or monitor this Interface. NNMi administrators and Level 2 Operators can use the drop-down selection list to change the current setting. **Note:** If you change the Direct Management Mode using **Actions** → **Management Mode**, NNMi updates the calculated Management Mode on the form. If you manually set the Direct Management Mode and then Save your changes, the Management Mode value is not updated until you refresh the form.
Hosted On Node	The 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,

Basic Attributes, continued

Attribute	Description
	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.
Physical Address	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.
Layer 2 Connection	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. 1. Navigate to the **Layer 2 Connection** attribute. Click the Lookup icon, and select Open. 2. In the Layer 2 Connection form, locate the **Interfaces** tab. 3. Double-click the row representing the other interface participating in this connection. 4. In the **Interface** form, locate the **Hosted On Node** attribute. 5. The Node form contains all known information about the neighboring node.

Interface State Attributes

Attribute	Description
Administrative State	The current Administrative State provided by: • The managing SNMP Agent • The managing Web Agent (*NNMi Advanced*) • Set by the device's administrator This value contributes towards the status calculation for this interface. See the "Interface Form: Status Tab" on page 140 for more information. Possible values are: **Up** – The interface is ready to pass packets of data. **Down** – The interface is not available to pass packets of data. **Testing** – The interface is in test mode. **Other** – The Administrative State reported is not a recognized value. The following values indicate NNMi could not gather the required data: **Agent Error** – Indicates an error was returned in response to the query. **No Polling Policy** - No polling policy exists for this monitored attribute. **Not Polled** - Indicates that this attribute is intentionally not polled, based on current

Interface State Attributes, continued

Attribute	Description
	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. **Not Provided** — The device does not support providing information for this monitored attribute. **Unavailable** - The agent responded with a value outside the range of possible values or returned a null value. **Unset** – Currently not used by NNMi.
Operational State	The current Operational State provided by: • The managing SNMP Agent • The managing Web Agent This value contributes towards the status calculation for this interface. See the "Interface Form: Status Tab" on page 140 for more information. Possible values are: **Up** – Ready to receive and send network traffic: the physical or virtual interface is operationally up. **Down** – The physical or virtual interface is operationally down. **Dormant** – Indicates interface is in a "pending" state, waiting for some external event. **Lower Layer Down** – Indicates the interface is down due to the state of lower-level interfaces. **Minor Fault** – The interface is still functional, but a minor concern was detected. Check the device, itself, for more details. **Not Present** – Indicates that the interface is missing. **Other** – The Operational State reported is not a recognized value. **Testing** – The interface is in test mode. **Unknown** – The Operational State value could not be detected. The following values indicate NNMi could not gather the required data: **Agent Error** – Indicates an error was returned in response to the query. **No Polling Policy** - No polling policy exists for this monitored attribute. **Not Polled** - 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.

Interface State Attributes, continued

Attribute	Description
	Not Provided — The device does not support providing information for this monitored attribute. **Unavailable** - The agent responded with a value outside the range of possible values or returned a null value. **Unset** – Currently not used by NNMi.
State Last Modified	(*NNMi Advanced - Global Network Management feature*) 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. The date and time when the Administrative State, Operational State, or both were last modified.
Notes	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. Type a maximum of 1024 characters. Alpha-numeric, spaces, and special characters (~ ! @ # $ % ^ & * ( ) _+ -) are permitted. **Note:** You can sort your interface table views based on this value. Therefore, you might want to include keywords for this attribute value.

Interface Form: General Tab

The "Interface Form" on page 113 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.
iIfAlias	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 (1.3.6.1.2.1.2.2.1.2) for the interface. This attribute is set by the device administrator.
ifIndex	Interface MIB variable for the row number in the interface table (ifTable)

General SNMP Values, continued

Attribute	Description
	for this interface. The row number can change. If you are an Administrator, see Accurately Detect Interface Changes for more information. **Note:** Interfaces on non-SNMP nodes have an ifIndex value of 0 (zero).
ifSpeed	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.
ifType	Interface MIB variable for the physical link protocol type of the interface. Possible values include: `Ethernet` and `frameRelay`. **Note:** Interfaces on non-SNMP nodes have an ifType value of `other`.
Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.	
Input Speed	(*NNM iSPI Performance for Metrics*) If the HPE 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. For example, you might want to override the Input Speed value for the following reason: 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). **Note:** (*NNMi Advanced - Global Network Management*) 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. If you are an NNMi administrator, you can set input speeds for multiple interfaces using the nnmsetiospeed.ovpl command. Also see

General SNMP Values, continued

Attribute	Description
	"Maintaining NNMi" in the HPE Network Node Manager i Software Deployment Reference for more information.
Output Speed	(*NNM iSPI Performance for Metrics*) If the HPE 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. For example, you might want to override the Output Speed value for the following reason: 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 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). **Note:** (*NNMi Advanced - Global Network Management*) 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. If you are an NNMi administrator, you can set output speeds for multiple interfaces using the nnmsetiospeed.ovpl command. Also see "Maintaining NNMi" in the *HPE Network Node Manager i Software Deployment Reference* for more information.

Interface Form: IP Addresses Tab

The "Interface Form" on page 113 provides details about the selected network interface.

For information about each tab:

IP Addresses Table

Attribute	Description
IP Address	Table view of the IP addresses associated with the selected interface. You can use this table to determine the state and address for each IP address. Double-click the row representing an IP address. The "IP Address Form" on page 160 displays all details about the selected IP address.

Interface Form: Ports Tab

The "Interface Form" on page 113 provides details about the selected network interface.

For information about each tab:

Ports Table

Attribute	Description
Ports	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. Double-click the row representing a port. The "Port Form" on page 229 displays all details about the selected port.

Interface Form: VLAN Ports Tab

Tip: The "Interface Form" on page 113 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

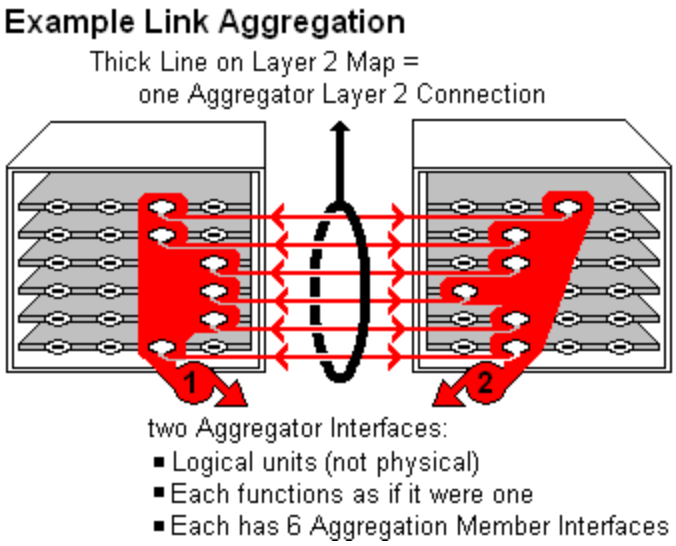
Attribute	Description
VLAN Ports	Table view of all of the VLAN ports associated with the current interface. Use this table to determine all port and VLAN combinations associated with this interface. Double-click the row representing a VLAN port. The "VLAN Port Form" on page 79 displays all details about the selected VLAN port.

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

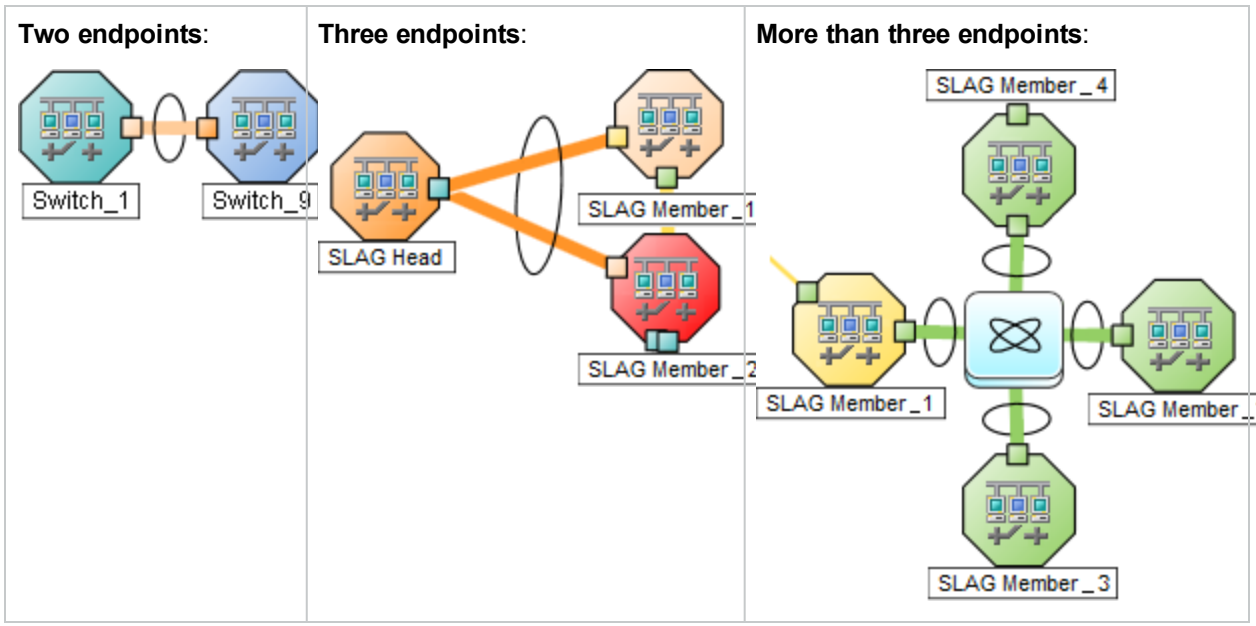
The "Interface Form" on page 113 provides details about the selected network interface.

For more information about each tab:

The Interface Form: Link Aggregation Tab appears if the selected interface uses a Link Aggregation protocol.



On a Layer 2 map, a thick line with a superimposed ellipse represents a **Link Aggregation**[1] or **Split Link Aggregation**[2] (group of multiple Layer 2 Connections that are functioning as one). The icon representing an Interface at either end of the thick line is an Aggregator Interface (a *logical* interface comprised of many physical interfaces that are functioning as one).



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

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

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

Attribute	Description
Link Aggregation Protocol	The **Link Aggregation**[1] or **Split Link Aggregation**[2] Protocol currently in use. These protocols allow network administrators to configure a *set of interfaces* on a switch as one *Aggregator Interface*, 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: **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 **Note:** 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 (/).
Aggregator	Name of the Aggregator that *contains* the selected participating Aggregation Member: • Aggregator Interface - represents multiple member interfaces • Aggregator Layer 2 Connection - thick line on the Layer 2 map represents multiple member Layer 2 Connections See Layer 2 Neighbor View Map Objects for more information. Click the Lookup icon, and choose Open to open the form for the Aggregator.

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

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

Attribute	Description
Link Aggregation Protocol	The **Link Aggregation**[1] or **Split Link Aggregation**[2] Protocol currently in use. These protocols allow network administrators to configure a *set of interfaces* on a switch as one *Aggregator Interface*, 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:
Available Bandwidth	Sum of the interface Input Speed attribute values of the Member Interfaces that have a MIB-II ifOperStatus that is not `Down`. 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.

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

Note: 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 (/).

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

Attribute	Description
Available Bandwidth Percentage	Percentage value computed using Available Bandwidth divided by the Maximum Bandwidth.
Members	Table view of the Aggregation Members. For more information, double-click the row representing an Aggregation Member: • The "Interface Form" on page 113 displays all details about the selected Interface. • The "Layer 2 Connection Form" on page 255 displays all details about the selected Layer 2 Connection.

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

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

The "Interface Form" on page 113 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 HPE 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:

- **High** - The High threshold was crossed.
- **Nominal** - Measured within healthy range. (Or no thresholds are being monitored.)
- **Low** - The Low threshold was crossed.
- **Abnormal Range** - This interface is abnormal based on the computed baseline for the specified threshold.
- **Normal Range** - This interface is normal based on the computed baseline for the specified threshold.

The following values indicate NNMi could not gather the required data:

- **Agent Error** – Indicates an error was returned in response to the query.
- **No Polling Policy** - No polling policy exists for this monitored attribute.
- **Not Polled** - 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

None - The value returned was zero.	polling policy. **Not Provided** — The device does not support providing information for this monitored attribute. **Unavailable** - The agent responded with a value outside the range of possible values or returned a null value. **Unset** – Currently not used by NNMi.

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**[1] value) compared to the total number of incoming frames. Possible causes include collisions at half-duplex, a duplex mismatch, bad hardware (**NIC**[2], 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**[3] value) compared to the total number of incoming frames. Possible causes include wireless communication interference, bad hardware (**NIC**[4], 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

[1]Cyclic Redundancy Check
[2]Network Interface Controller
[3]Cyclic Redundancy Check
[4]Network Interface Controller

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 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: IP Addresses Tab

The "Interface Form" on page 113 provides details about the selected network interface.

For information about each tab:

IP Addresses Table

Attribute	Description
IP Address	Table view of the IP addresses associated with the selected interface. You can use this table to determine the state and address for each IP address. Double-click the row representing an IP address. The "IP Address Form" on page 160 displays all details about the selected IP address.

Interface Form: Capabilities Tab

The "Interface Form" on page 113 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 to access information about each Capability. Double-click the row representing a Capability. The "Interface Capability Form" on page 134 displays all details about the selected Capability. For more information, see "Interface Capabilities Provided by NNMi" below.

Interface Capabilities Provided by NNMi

The "Interface Form: Capabilities Tab" above 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.

Additional vendor-specific capabilities may appear from device extension settings.

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*> = chassis, card, ipaddr (address), iface (interface), lag (**Link Aggregation**[1] or **Split Link Aggregation**[2] interface), node, rrp (Router Redundancy), or metric (Node Sensor or Physical Sensor).

<*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
com.hp.nnm.capability.iface.private	Private	Indicates the interface was discovered in either a non-SNMP node or a Nortel node. Private interfaces are not monitored for Status. 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).

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

Interface Capability Attribute Values, continued

Unique Key	Capability	Description
		• 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. 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.
`com.hp.nnm.capability.iface.ietf.NON-DEFAULT-CONTEXT-RFC1213`	RFC 1213 Interface from Non-default Context	Indicates the following: • NNMi discovered the interface from the RFC1213 MIB. • The interface has a context other than default. **Note:** • NNMi collects context values using the vacmContextTable in the SNMP-VIEW-BASED-ACM-MIB defined in RFC2575. • NNMi does not monitor interfaces under a non-default context.
`com.hp.nnm.capability.iface.PE`	PE Interface	Indicates that the interface is

Interface Capability Attribute Values, continued

Unique Key	Capability	Description
		serving as a Provider Edge (**PE**[1]). NNMi's Subnet Connection Rules use this information.
com.hp.nnm.capability.br.bridge	Virtual Bridge	Indicates that the interface represents a virtual bridge (also known as a virtual switch).
com.hp.nnm.capability.br.port	Virtual Bridge Port	Indicates that the interface represents any interface associated with a virtual bridge.
	VM Virtual Machine Interface	
Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.		
com.hp.nnm.capability.iface.ietf.DS1	DS1 Interface Metrics	Interface that supports the DS1 (T1) MIB for gathering performance data. This data is used by NNM iSPI Performance for Metrics.
com.hp.nnm.capability.iface.ietf.DS3	DS3 Interface Metrics	Interface that supports the DS3 (T3) MIB for gathering performance data. This data is used by NNM iSPI Performance for Metrics.
com.hp.nnm.capability.iface.ietf.ETHERLIKE	EtherLike Interface Metrics	Interface that supports the Etherlike MIB for gathering performance 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

[1]Provider Edge router. The Internet Service Provider's router that receives your data on the path to your data's final desination. The Customer Edge (CE) router in your network connects to this PE.

Interface Capability Attribute Values, continued

Unique Key	Capability	Description
		Metrics.
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	Indicates the interface is an IPv6 interface, *discovered using only the RFC 2465 IPv6-MIB and **not** the standard RFC 2863 IF-MIB*. 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*>]).

(*NNMi Advanced*) The capabilities in the following table identify how the interface is participating in a **Link Aggregation**[1] or **Split Link Aggregation**[2].

(*NNMi Advanced*) Link Aggregation Interface Capabilities: Roles

Unique Key	Capability	Description
`com.hp.nnm.capability.lag.aggregator`	Aggregator Interface	Indicates the interface represents a collection of participating interfaces at one end of an Aggregator Layer 2 Connection. See Layer 2 Neighbor View Map Objects for more information.
`com.hp.nnm.capability.lag.member`	Aggregation Member	Indicates the interface is a physical interface that is a member of an Aggregator Interface. See Layer 2 Neighbor View Map Objects for more information.

(*NNMi Advanced*) The capabilities in the following table are used when **Link Aggregation**[3] or **Split Link Aggregation**[4] protocol is available.

(*NNMi Advanced*) Link Aggregation Interface Capabilities: Protocols

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

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.
[3]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).
[4]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

(NNMi Advanced) Link Aggregation Interface Capabilities: Protocols, continued

Unique Key	Capability	Description
`com.hp.nnm.capability.lag.protocol.mlt`	Nortel Multi-Link Trunking	Nortel Multi-Link Trunk technology (mlt)
`com.hp.nnm.capability.lag.protocol.istmlt`	Inter-Switch Trunk MLT	Split Multi-Link Trunk: inter-switch trunk (istMlt)
`com.hp.nnm.capability.lag.protocol.smlt`	Split MLT	Split Multi-Link Trunk: configuration technology (splitMlt)
`com.hp.nnm.capability.lag.protocol.unknown`	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 128 shows a list of all available Capabilities for that interface. For more information, see "Interface Capabilities Provided by NNMi" on page 128.
Unique Key	Used as a unique identifier for the Capability. Any capability provided by NNMi begins with the prefix `com.hp.nnm.capability`. For more information, see "Interface Capabilities Provided by NNMi" on page 128.

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. See "Custom Interface

Attribute Samples" on page 136.

The Interface Form: Custom Attributes tab displays a table view of any Custom Attributes that have been added to the selected interface.

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 can be replicated from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager configure which Regional Custom Attributes they want (Global Manager: Configure Custom Attribute Replication). NNMi administrators can also configure Custom Attribute values that are unique to the Global Manager's environment (Customize Object Attributes).

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. Limit 50 of any combination of keyboard entries including spaces.
Value	The actual value for the Custom Attribute for the selected interface. Limit 2,000 of any combination of keyboard entries including spaces. For more information, see "Custom Interface Attributes Form" below.

Custom Interface Attributes Form

Custom Attributes enable an NNMi administrator to add information to a node object. Custom Attributes can also be set by external applications that have been integrated with NNMi. See "Custom Interface Attribute Samples" on the next page.

The required settings for these attributes are described in the table below.

(*NNMi Advanced - Global Network Management feature*) Custom Attribute values can be replicated from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager configure which Regional Custom Attributes they want (Global Manager: Configure Custom Attribute Replication). NNMi administrators can also configure Custom Attribute values that are unique to the Global Manager's environment (Customize Object Attributes).

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. Limit 50 of any combination of keyboard entries including spaces.
Value	Value assigned to the Custom Attribute for the selected interface object. Limit 2,000 of any combination of keyboard entries including spaces. For more information, see "Interface Form: Custom Attributes Tab" on the previous page.

Custom Interface Attribute Samples

Custom Attributes provide additional information about an object instance:

- NNMi administrators can associate custom information with the Interface for their network management team's benefit.

  For example, your NNMi administrator might have added the following:

  - **Name**: `Assignment`
  - **Value**: `WAN interface to the London office.`

- External applications that have been integrated with NNMi can associate custom information with the Interface.

  For example, when *HPE Network Node Manager iSPI Performance for Metrics Software* is installed, your NNMi administrator can provide additional Node or Interface information in NNM iSPI Performance for Metrics reports:

  - **Name** = `NPS Annotation`
  - **Value** = <*text to appear in the reports*>.

  See the help topic: Annotate NNM iSPI Performance for Metrics Reports.

- NNMi can associate custom information about an Interface.

  For example, if the NNMi administrator enables the Discovery and Monitoring of unnumbered interfaces, you will see this Custom Attribute associated with each unnumbered interface:

  - **Name**: `UnnumberedNextHop`
  - **Value**: <*IP address of the neighboring device*>

(*NNMi Advanced - Global Network Management feature*) Custom Attribute values can be replicated from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager configure which Regional Custom Attributes they want (Global Manager: Configure Custom Attribute Replication). NNMi administrators can also configure Custom Attribute values that are unique to the Global Manager's environment (Customize Object Attributes).

Related Topics:

"Interface Form: Custom Attributes Tab" on page 134

"Custom Interface Attributes Form" on the previous page

Interface Form: Interface Groups Tab

The "Interface Form" on page 113 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 302 displays all details about the selected Interface Group.

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

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

The "Interface Form" on page 113 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 HPE 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:

- **High** - The High threshold was crossed.
- **Nominal** - Measured within healthy range. (Or no thresholds are being monitored.)
- **Low** - The Low threshold was crossed.
- **None** - The value returned was zero.

- **Abnormal Range** - This interface is abnormal based on the computed baseline for the specified threshold.
- **Normal Range** - This interface is normal based on the computed baseline for the specified threshold.

The following values indicate NNMi could not gather the required data:

- **Agent Error** – Indicates an error was returned in response to the query.
- **No Polling Policy** - No polling policy exists for this monitored attribute.
- **Not Polled** - 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.
- **Not Provided** — The device does not support providing information for this monitored attribute.
- **Unavailable** - The agent responded with a value outside the range of possible

	values or returned a null value. **Unset** – Currently not used by NNMi.

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**[1] value) compared to the total number of incoming frames. Possible causes include collisions at half-duplex, a duplex mismatch, bad hardware (**NIC**[2], 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**[3] value) compared to the total number of incoming frames. Possible causes include wireless communication interference, bad hardware (**NIC**[4], 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

[1]Cyclic Redundancy Check
[2]Network Interface Controller
[3]Cyclic Redundancy Check
[4]Network Interface Controller

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 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 113 provides details about the selected network interface.

For information about each tab:

Incidents Table

Attribute	Description
Associated	Table view of the incidents associated with the selected interface. These incidents are sorted

Incidents Table, continued

Attribute	Description
Incidents	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. Double-click the row representing an incident. The "Incident Form" on page 437 displays all details about the selected incident.

Interface Form: Status Tab

The "Interface Form" on page 113 provides details about the selected network interface.

For information about each tab:

Status Tab

Attribute	Description
Status	Overall status for the current interface. NNMi follows the ISO standard for status classification. Possible values are: **Note:** The icons are displayed only in table views. No Status Normal Disabled Unknown Warning Minor Major Critical Interface status is derived from SNMP polling results for ifAdminStatus and IfOperStatus, 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 406 for more information about possible status values. (*NNMi Advanced*)

Status Tab, continued

Attribute	Description
	• **Link Aggregation**[1] or **Split Link Aggregation**[2]: 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 121 and Status Color for Link Aggregation Objects. • If the interface is a virtual interface, note that the following categories indirectly indicate the current condition of the **hypervisor**[3]: Indicates that the hypervisor is Up Indicates that the hypervisor is Down Indicates a Null value in hypervisor state
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 113 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:

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.
[3]The virtual machine manager in charge of delegating various aspects from a pool of resources to become virtual devices. The delegations might be static or dynamic, depending on the manufacture's implementation. The type of virtual machines being generated depends on the manufacturer's implementation.

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. 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. The Status value is correlated based on the most critical Conclusions. Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion. The following table describes the possible Conclusions that might appear for an interface object. **Note:** A **Y** in the **Incident?** column indicates that the Conclusion results in an incident. **Critical Status Conclusions** **Conclusion** / **Description** / **Status** / **Incident?** AggregatorDown / **Link Aggregation**[1] or **Split Link Aggregation**[2]: 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 121. / Critical / Y InterfaceDown / The interface Operational State is Down. / Critical / Y **Major Status Conclusions** (*NNM iSPI Performance for Metrics*) **Conclusion** / **Description** / **Status** / **Incident?** InterfaceFCSLANErrorRateHigh / *Local Area Network*. Indicates a Frame Check Sequence (FCS) error rate on the / Major / Y

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

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**[1] value). Possible causes include collisions at half-duplex, a duplex mismatch, bad hardware (**NIC**[2], cable, or port), or a connected device generating frames with bad FCS.		
InterfaceFCSWLANErrorRateHigh	*Wireless Local Area Network*. 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**[3] value). Possible causes include collisions at half-duplex, a duplex mismatch, bad hardware (**NIC**[4], cable, or port), or a connected device generating frames with bad FCS.	Major	Y
InterfaceInputDiscardRateHigh	The input discard rate on the interface has	Major	Y

[1]Cyclic Redundancy Check
[2]Network Interface Controller
[3]Cyclic Redundancy Check
[4]Network Interface Controller

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	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.		
InterfaceInputErrorRateHigh	The input error 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 packet error count.	Major	Y
InterfaceInputQueueDropsRateHigh	The number of input queue drops on the interface has exceeded a threshold setting. This range is based on the number of 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.	Major	Y
InterfaceInputUtilizationHigh	The input utilization on the interface has exceeded a threshold setting. This percentage is based on the interface speed and the reported	Major	Y

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	change in the number of input bytes on the interface.		
InterfaceInputUtilizationLow	The input 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 input bytes on the interface.	Major	Y
InterfaceInputUtilizationNone	The input utilization for the interface is zero (0). This value is based on the interface speed and the reported change in the number of input bytes on the interface.	Major	Y
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

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
InterfaceOutputQueueDropsRateHigh	The number of output queue drops on the interface has exceeded a threshold setting. This number is based on the number of packets dropped because of a full queue.	Major	Y
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 interface speed and the reported change in the number of output bytes on the interface.	Major	Y

Minor Status Conclusions

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
AggregatorDegraded	**Link Aggregation**[1] or **Split Link Aggregation**[2]: 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 "Interface Form: Link Aggregation Tab (NNMi Advanced)" on page 121.	Minor	Y
vSwitchDegraded	(NNMi Advanced). The Operational State of the virtual switch is Down. This occurs when the Operational State of all uplinks on the virtual switch is Down.	Minor	N

Warning Status Conclusions (*NNM iSPI Performance for Metrics*)

Conclusion	Description	Status	Incident?
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 bytes on the interface.	Warning	Y
InterfaceOutputUtilizationAbnormal	The output utilization on the interface is abnormal based on the computed baseline.	Warning	Y

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	This range is based on the interface speed, and the reported change in the number of output bytes on the interface.		

Warning Status Conclusions (NNMi Advanced)

Conclusion	Description	Status	Incident?
vSwitchWarning	The Operational State of at least one uplink on the virtual switch is Down.	Warning	N

Disabled Status Conclusions

Conclusion	Description	Status	Incident?
InterfaceDisabled	The interface has been explicitly disabled by the device administrator.	Disabled	Y
vSwitchDisabled	(NNMi Advanced). The Administrative State of the virtual switch is Down. This occurs when the Administrative State of all of the uplinks associated with the virtual switch is Down.	Disabled	N

Unknown Status Conclusions

Conclusion	Description	Status	Incident?
InterfaceUnmanagable	The agent associated with the interface is not responding to queries.	Unknown	N

Normal Status Conclusions

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
AggregatorUp	**Link Aggregation**[1] or **Split Link Aggregation**[2]: The Aggregator 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 121.	Normal	N
vSwitchUp	(NNMi Advanced). Indicates the Operational State of the virtual switch is Up. This occurs when the Operational State of all uplinks on the virtual switch is Up.	Normal	N
Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.			
InterfaceEnabled	The interface has	Normal	N

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	an Administrative State of Up.		
InterfaceFCSLANErrorRateInRange	(*NNM iSPI Performance for Metrics*) The Frame Check Sequence error rate for the interface is within the allowable range set by the administrator.	Normal	N
InterfaceFCSWANErrorRateInRange	(*NNM iSPI Performance for Metrics*) The Frame Check Sequence error rate for the interface is within the allowable range set by the administrator.	Normal	N
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

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
InterfaceInputDiscardRateNone	(*NNM iSPI Performance for Metrics*) The input discard rate for the interface is zero (0) .	Normal	N
InterfaceInputErrorRateLow	(*NNM iSPI Performance for Metrics*) The input error rate for the interface is below the allowable threshold range set by the administrator.	Normal	N
InterfaceInputErrorRateNominal	(*NNM iSPI Performance for Metrics*) The input error rate for the interface is within the allowable threshold range set by the administrator.	Normal	N
InterfaceInputErrorRateNone	(*NNM iSPI Performance for Metrics*) The input error rate for the interface is zero (0).	Normal	N
InterfaceInputQueueDropsRateInRange	(*NNM iSPI Performance for Metrics*) 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	(*NNM iSPI Performance for Metrics*) The input utilization for the interface is within the allowable threshold range set by the administrator.	Normal	N
InterfaceInputUtilizationNormal	(*NNM iSPI Performance for Metrics*) 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	(*NNM iSPI Performance for Metrics*) The output discard rate for the interface is below the allowable threshold range set by the administrator.	Normal	N
InterfaceOutputDiscardRateNominal	(*NNM iSPI Performance for Metrics*) The output discard rate for the interface is within the allowable threshold range set by the	Normal	N

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	administrator.		
InterfaceOutputDiscardRateNone	(*NNM iSPI Performance for Metrics*) The output discard rate for the interface is zero (0).	Normal	N
InterfaceOutputErrorRateLow	(*NNM iSPI Performance for Metrics*) The output error rate for the interface is below the allowable low range set by the administrator.	Normal	N
InterfaceOutputErrorRateNominal	(*NNM iSPI Performance for Metrics*) The output error rate for the interface is within the allowable threshold range set by the administrator.	Normal	N
InterfaceOutputErrorRateNone	(*NNM iSPI Performance for Metrics*) The output error rate for the interface is zero (0).	Normal	N
InterfaceOutputQueueDropsRateInRange	(*NNM iSPI Performance for Metrics*) The number of output queue drops for the interface is within the allowable threshold range set by the administrator.	Normal	N

Outstanding Status Conclusion Values, continued

Attribute	Description
	<table><tr><th>Conclusion</th><th>Description</th><th>Status</th><th>Incident?</th></tr><tr><td>InterfaceOutputUtilizationNominal</td><td>(*NNM iSPI Performance for Metrics*) The output utilization for the interface is within the allowable threshold range set by the administrator.</td><td>Normal</td><td>N</td></tr><tr><td>InterfaceOutUtilizationNormal</td><td>(*NNM iSPI Performance for Metrics*) The output utilization for the interface is within the allowable threshold range set by the administrator.</td><td>Normal</td><td>N</td></tr><tr><td>InterfaceUp</td><td>The Operational State of the interface is Up.</td><td>Normal</td><td>N</td></tr></table>

Interface Form: Registration Tab

The "Interface Form" on page 113 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. **Note:** This value does not change when a node is rediscovered. This is because the Node object is modified, but not created.
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. Note the following: • When a node is rediscovered, the Last Modified time is the same as the Discovery

Registration Attributes, continued

Attribute	Description
	Completed time. This is because the node's Discovery State changes from Started to Completed. • 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.

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.

Virtual Switch's Interface Form (NNMi Advanced)

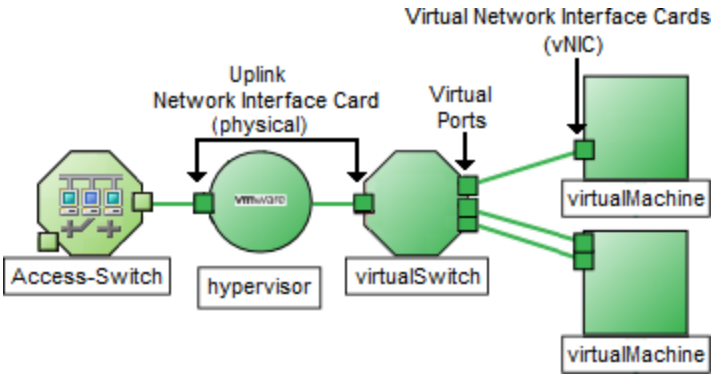
When the "Interface Form" on page 113 provides details about a virtual switch, two additional tabs appear:

- **Uplinks**
- **Virtual Ports**

The virtual switch is identified with the **Virtual Bridge** capability (see "Interface Form: Capabilities Tab" on page 128).

You can launch the virtual switch's Interface form from the following locations:

- A table of Interfaces
- A map view by double-clicking the Switch icon



For additional information about the **hypervisor**[1] providing this virtual switch, see:

- Using the Wheel Dialog
- Using the Loom Dialog

[1]The virtual machine manager in charge of delegating various aspects from a pool of resources to become virtual devices. The delegations might be static or dynamic, depending on the manufacture's implementation. The type of virtual machines being generated depends on the manufacturer's implementation.

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 `ifName` value. Second choice is the `ifAlias` value. Third choice is a combination of the `ifType[ifIndex]` value (for example, `ethernetCsmacd[17]`).
Status	Overall status for the current interface. NNMi follows the ISO standard for status classification. See the "Interface Form: Status Tab" on page 140 for more information. Possible values are: No Status Normal Disabled Unknown Warning Minor Major Critical Interface status is derived from SNMP polling results for ifAdminStatus and IfOperStatus, as well as from any conclusions. Status reflects the most serious outstanding conclusion. See the "Interface Form: Conclusions Tab" on page 141 for information about how the current status was determined. See "Watch Status Colors" on page 406 for more information about possible status values. **Note:** The icons are displayed only in table views.
Management Mode	The *calculated* Management Mode for the interface according to the Management Mode Hierarchy. This value reflects the current management mode of this interface's parent object (the Hosted On Node). See "How NNMi Assigns the Management Mode to an Object" on page 591. (*NNMi Advanced - Global Network Management feature*) 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. **Note:** If the NNMi Security configuration permits, you can change this setting using **Actions** → **Management Mode**. **Tip:** You can also right-click any object in a table or map view to access the items available within the **Actions** menu.

Basic Attributes, continued

Attribute	Description
Direct Management Mode	Indicates whether or not NNMi is currently monitoring the interface. Possible values are: **Inherited** – Used to indicate that the interface should inherit the Management Mode from this interface's parent object (the Hosted On Node). **Not Managed** – 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. **Out of Service** – Used to indicate an interface is unavailable because it is out of service or participating in a Scheduled Node Outage. NNMi does not discover or monitor this Interface. NNMi administrators and Level 2 Operators can use the drop-down selection list to change the current setting. **Note:** If you change the Direct Management Mode using **Actions** → **Management Mode**, NNMi updates the calculated Management Mode on the form. If you manually set the Direct Management Mode and then Save your changes, the Management Mode value is not updated until you refresh the form.
Hosted On Node	The 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 administrator configured the discovery process). Click the Lookup icon and select Show Analysis or Open to display more information about the node.
Physical Address	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.
Layer 2 Connection	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. 1. Navigate to the **Layer 2 Connection** attribute. Click the Lookup icon, and select Open. 2. In the Layer 2 Connection form, locate the **Interfaces** tab. 3. Double-click the row representing the other interface participating in this connection. 4. In the **Interface** form, locate the **Hosted On Node** attribute. 5. The Node form contains all known information about the neighboring node.

Interface State Attributes

Attribute	Description
Administrative	The current Administrative State provided by:

Interface State Attributes, continued

Attribute	Description
State	• The managing SNMP Agent • The managing Web Agent (*NNMi Advanced*) • Set by the device's administrator This value contributes towards the status calculation for this interface. See the "Interface Form: Status Tab" on page 140 for more information. Possible values are: **Up** – The interface is ready to pass packets of data. **Down** – The interface is not available to pass packets of data. **Testing** – The interface is in test mode. **Other** – The Administrative State reported is not a recognized value. The following values indicate NNMi could not gather the required data: **Agent Error** – Indicates an error was returned in response to the query. **No Polling Policy** - No polling policy exists for this monitored attribute. **Not Polled** - 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. **Not Provided** — The device does not support providing information for this monitored attribute. **Unavailable** - The agent responded with a value outside the range of possible values or returned a null value. **Unset** – Currently not used by NNMi.
Operational State	The current Operational State provided by: • The managing SNMP Agent • The managing Web Agent (*NNMi Advanced*) This value contributes towards the status calculation for this interface. See the "Interface Form: Status Tab" on page 140 for more information. Possible values are: **Up** – The interface is operationally up, ready to receive and send network traffic. **Down** – The interface is operationally down. **Dormant** – Indicates interface is in a "pending" state, waiting for some external event. **Lower Layer Down** – Indicates the interface is down due to the state of lower-level interfaces.

Interface State Attributes, continued

Attribute	Description
	Minor Fault – The interface is still functional, but a minor concern was detected. Check the device, itself, for more details. **Not Present** – Indicates that the interface is missing. **Other** – The Operational State reported is not a recognized value. **Testing** – The interface is in test mode. **Unknown** – The Operational State value could not be detected. The following values indicate NNMi could not gather the required data: **Agent Error** – Indicates an error was returned in response to the query. **No Polling Policy** - No polling policy exists for this monitored attribute. **Not Polled** - 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. **Not Provided** — The device does not support providing information for this monitored attribute. **Unavailable** - The agent responded with a value outside the range of possible values or returned a null value. **Unset** – Currently not used by NNMi.
State Last Modified	(*NNMi Advanced - Global Network Management feature*) 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. The date and time when the Administrative State, Operational State, or both were last modified.
Notes	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. Type a maximum of 1024 characters. Alpha-numeric, spaces, and special characters (~ ! @ # $ % ^ & * ( ) _+ -) are permitted. **Note:** You can sort your interface table views based on this value. Therefore, you might want to include keywords for this attribute value.

Interface Form: Uplinks Tab (NNMi Advanced)

The Interface Form provides details about the selected interface.

Tip: The **Uplinks** tab appears only for those interfaces that represent virtual switches. Use this tab to view the list of physical interfaces associated with that virtual switch. These interfaces are identified using the **Virtual Bridge Port** capability.

For information about each tab:

Uplinks Table

Attribute	Description
Interfaces	Table view of all of the interfaces representing the uplink associated with the virtual switch. Double-click the row representing an interface. The "Interface Form" on page 113 displays all details about the selected interface.

Interface Form: Virtual Ports Tab (NNMi Advanced)

The "Interface Form" on page 113 provides details about the selected network interface.

Tip: The **Virtual Ports** tab appears only for those interfaces that represent virtual switches. Use this tab to view the list of virtual interfaces on the virtual switch that connect to **virtual machine**[1] nodes. Virtual Ports are identified using the **Virtual Bridge Port** capability.

For information about each tab:

Virtual Ports Table

Attribute	Description
Ports	Table view of all of the virtual interfaces that connect to a virtual switch. Use this table to access information about each virtual interface associated with the selected virtual switch. Double-click the row in the Virtual Ports table. The "Interface Form" on page 113 displays all details about the selected virtual interface that is acting as a virtual port.

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.

[1]A device that utilizes components from multiple physical devices. Depending on the manufacture's implementation, the virtual machine may be static or dynamic.

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 *static* Network Address Translation (NAT) is part of your network management domain, your NNMi administrator can configure NNMi to display the NAT *internal IP address* (such as private IPv4 address) assigned to the selected *external IP address*.
Status	Overall status for the current IP address. NNMi follows the ISO standard for status classification. See "IP Address Form: Status Tab" on page 166.
Management Mode	The *calculated* Management Mode for the address according to the Management Mode Hierarchy. This value reflects the current management mode of this IP address's parent object (either an Interface or the Hosted On Node). See "How NNMi Assigns the Management Mode to an Object" on page 591. (*NNMi Advanced - Global Network Management feature*) 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. **Note:** If the NNMi Security configuration permits, you can change this setting using **Actions** → **Management Mode**. **Tip:** You can also right-click any object in a table or map view to access the items available within the **Actions** menu.
Direct Management Mode	Indicates whether or not NNMi is currently monitoring the IP address. Possible values are: **Inherited** – Used to indicate that the address should inherit the Management Mode from the address's parent object (either the Parent Component interface or the Managed By node). **Not Managed** – 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. **Out of Service** – Used to indicate the address is unavailable because it is out of service or participating in a Scheduled Node Outage. NNMi does not discover or monitor this address. NNMi administrators and Level 2 Operators can use the drop-down selection list to change the current setting.

Basic Attributes, continued

Attribute	Description
	Note: If you change the Direct Management Mode using **Actions → Management Mode**, NNMi updates the calculated Management Mode on the form. If you manually set the Direct Management Mode and then Save your changes, the Management Mode value is not updated until you refresh the form.
State	Indicates whether NNMi is communicating with the IP address. Possible values are: **Responding** – Indicates that the IP address is being polled and is responding to an ICMP ping. **Not Responding** – Indicates that the IP address is being polled, but is not responding to an ICMP ping. The following values indicate NNMi could not gather the required data: **No Polling Policy** - No polling policy exists for this monitored attribute. **Not Polled** - 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. **Not Provided** — The device does not support providing information for this monitored attribute. **Unavailable** - The agent responded with a value outside the range of possible values or returned a null value. **Unset** – Currently not used by NNMi. **Note:** NNMi's State Poller determines the State. The current state contributes towards the status calculation for the address. See the Status tab for more information.
State Last Modified	The date and time when the State value was last modified.
In Interface	MIB-II ipAddrTable value indicating the interface that owns this IP address. Click the Lookup icon and select Open to display more information about the interface.
Hosted On Node	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

Basic Attributes, continued

Attribute	Description
	and the subnet prefix information. Click the Lookup icon and select Open to display more information about the IP subnet.
Notes	(*NNMi Advanced - Global Network Management feature*) 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. **Note:** 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 437 for more details about the incident attributes that appear in the incident view's column headings.

The "IP Address Form" on page 160 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 437 displays all details about the selected incident.

IP Address Form: Capabilities Tab

The "IP Address Form" on page 160 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**[1] 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	Table of all of the capabilities associated with the selected IP Address. Use this table to access information about each Capability. Double-click the row representing a Capability. The "IP Address Capability Form" on the next page displays all details about the selected Capability. For more information, see "IP Address Capabilities Provided by NNMi" below.

IP Address Capabilities Provided by NNMi

The "IP Address Form: Capabilities Tab" on the previous page 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.

<*content*> = chassis, card, ipaddr (address), iface (interface), lag (**Link Aggregation**[2] or **Split Link Aggregation**[3] interface), node, rrp (Router Redundancy), or metric (Node Sensor or Physical Sensor).

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

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

[1]Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.
[2]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).
[3]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

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 **loopback address**[1].
`com.hp.nnm.capability.address.anycast`	ANYCAST	Used to identify an address that is either of the following: • IPv4 **Anycast Rendezvous Point IP Address**[2] that are loopback addresses used for routers in multi-cast network configurations. These duplicate IP addresses are excluded from monitoring. • (NNMi Advanced) IPv6 Anycast address.
`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**[3] 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.

[1]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.
[2]Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.
[3]Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

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 163 shows a list of all available Capabilities for that IP address. For more information, see "IP Address Capabilities Provided by NNMi" on page 164.
Unique Key	Used as a unique identifier for the Capability. Any capability provided by NNMi begins with the prefix `com.hp.nnm.capability`. For more information, see "IP Address Capabilities Provided by NNMi" on page 164.

IP Address Form: Status Tab

The "IP Address Form" on page 160 provides details about the selected IP address .

For information about each tab:

Status of this IP Address

Attribute	Description
Status	Overall status for the current IP address. NNMi follows the ISO standard for status classification. Possible values are: No Status Normal Disabled Unknown Warning Minor Major Critical 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 "IP Address Form: Conclusions Tab" on the next page. Status reflects the most serious outstanding conclusion. See "Watch Status Colors" on page 406 for more information about possible status values. **Note:** The icons are displayed only in table views.
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 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. Double-click the row representing a Status History. The Status History form displays all details about the selected Status.

IP Address Form: Conclusions Tab

The "IP Address Form" on page 160 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	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. Each Conclusion listed is still outstanding and applies to the current overall Status. This view is useful for obtaining a quick summary of the Status and problem description for the current node's IP address that led up to the address' most current Status. The Status value is correlated based on the most critical Conclusions. Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion. The following table describes the possible Conclusions that might appear for an IP Address object. **Note:** A **Y** in the **Incident?** column indicates that the Conclusion results in an incident. **Critical Status Conclusions** **Conclusion** / **Description** / **Status** / **Incident?** AddressNotResponding / The address is not responding to ICMP ping. / Critical / Y **Normal Status Conclusions**

Outstanding Status Conclusion Values, continued

Attribute	Description
	<table><tr><th>Conclusion</th><th>Description</th><th>Status</th><th>Incident?</th></tr><tr><td>AddressResponding</td><td>The address responds to ICMP ping.</td><td>Normal</td><td>N</td></tr></table>

IP Address Form: Registration Tab

The "IP Address Form" on page 160 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. **Note:** This value does not change when a node is rediscovered. This is because the Node object is modified, but not created.
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. Note the following: • 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. • 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.

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	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. 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. • 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). When the NNMi administrator chooses **Enable SNMP Address Rediscovery** ☑ in the Communication Configuration: ◦ If the SNMP Agent does not respond, NNMi checks for another Management Address to request the Hostname, and the Hostname could change. ◦ If the SNMP Agent associated with the node changes, the Management Address and Hostname could change. When the NNMi administrator disables **Enable SNMP Address Rediscovery** ☐ in the Communication Configuration, when the current management address (SNMP agent) becomes unreachable, NNMi does not check for other potential management addresses. • 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. **Note:** NNMi administrators can use NNMi property file settings to change the way NNMi determines Hostname values: • `nms-topology.properties` 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 *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`. • `nms-disco.properties` 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 *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.

Basic Attributes, continued

Attribute	Description
* Mode	*NNMi administrators only*. Click here for more information. Enables you to specify how NNMi determines the values of the editable Attributes within this instance of the SNMP Agent form. **Note:** When the node is first discovered, the SNMP Agent's Mode = **Auto** by default. NNMi discovers and monitors Nodes using the Communication Configuration settings. See Configuring Communication Protocol for more information. **SNMP Agent Settings Mode Options** **Option** / **Description** **Auto** — NNMi uses the current appropriate Communication Configuration settings to determine the values of the Attributes within this instance of the SNMP Agent form. See Configuring Communication Protocol for more information. **Locked** — The NNMi Administrator controls the values of the *editable* Attributes within this instance of the SNMP Agent form for discovery and monitoring. Any future updates to those configuration settings must be established within this instance of the SNMP Agent form. **Tip:** You can also use nnmcomunication.ovpl to set the Mode and view this SNMP Agent's configuration settings.
Management Address	IP address NNMi uses to communicate with this SNMP agent. **Note:** As an NNMi administrator, you can over-ride this setting and specify the management address on a per-node basis using the SNMP Agent Form. The IP address you enter must be a valid IP address for the associated Node. Also see the **Mode** attribute description. **Tip:** If you are an NNMi administrator, you can also use nnmcomunication.ovpl to change the **Management Address** value and to view the SNMP Agent settings. The NNMi administrator can specify an address or NNMi can dynamically select one. Click here for details. **Note:** (*NNMi Advanced*) The NNMi administrator specifies whether NNMi prefers IPv4 addresses, IPv6 addresses, or dual-stack (both) when selecting the Management Address. See Configure Default SNMP, Management Address, and ICMP Settings.

Basic Attributes, continued

Attribute	Description
	1. NNMi ignores the following addresses when determining which Management Address is most appropriate: • Any address of an administratively-down interface. • Any address that is virtual (for example, **VRRP**[1]). • Any IPv4 **Anycast Rendezvous Point IP Address**[2] or IPv6 Anycast address. • Any address in the reserved loopback network range. IPv4 uses 127/24 (`127.*.*.*`) and IPv6 uses `::1`. • Any **IPv6 link-local address**[3]. 2. If the NNMi Administrator chooses **Enable SNMP Address Rediscovery** ☑ in Communication Configuration, NNMi prefers the last-known Management Address (if any). 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 *Management Address Selection*. The NNMi Administrator chooses the order in which NNMi checks the following: • 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. • Lowest Loopback - If a node supports multiple **loopback address**[4], 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).

[1]Virtual Router Redundancy Protocol
[2]Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.
[3]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.
[4]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
	• Highest Loopback - If a node supports multiple **loopback address**[1], 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. • Interface Matching - The NNMi Administrator chooses which interface MIB variable NNMi queries to detect changes. NNMi can use the following MIB-II attribute values: `ifIndex`, `ifName`, `ifDescr`, `ifAlias`, or a combination of these (`ifName` or `ifDescr`, `ifName` or `ifDescr` or `ifAlias`). NNMi searches current database entries for information about the interface in this order: index, alias, name, and description. If multiple IP addresses are associated with the interface, NNMi starts by querying the lowest IP address and selects the first responding address in ascending order. 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. 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). **Note:** The address represents a *static* Network Address Translation (NAT) pair's *external IP address* 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. 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 *SNMP Minimum Security Level* settings). 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. 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 **Enable SNMP Address Rediscovery** ☐ (disabled) or *Preferred Management Address* setting.

[1]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	The *read community string* value that was discovered for the selected SNMP agent. Note the following: • The read community string is an SNMPv1 or SNMPv2c password. • The actual read community string is only visible if you are assigned to the NNMi administrator role. • If you are an NNMi administrator, you can change this value for the selected SNMP Agent and its associated node. • The NNMi administrator can also choose to make this value viewable (read only) to Level 2 Operators. If you are an NNMi administrator, see the "Maintaining NNMi" chapter of the HPE Network Node Manager i Software Deployment Reference for more information.
SNMP Agent Enabled	Indicates whether this SNMP agent is set up for SNMP communication in your network environment. **Note:** When an agent is Disabled, any data previously reported by that agent is preserved in the NNMi database. Data reported by an Enabled agent is updated as new data is received.
UDP Port	User Datagram Protocol port configuration for this SNMP agent. Default 161. Port NNMi is instructed to use when contacting this SNMP agent to collect SNMP data. Both the Discovery Process and the State Poller Service use this setting.
Get-Bulk Enabled	*Applies only to SNMPv2 or higher.* If you have devices in your network environment that have trouble responding to `GetBulk` commands, you can instruct NNMi to use `Get` or `GetNext` instead of `GetBulk`. If ☑ enabled, NNMi uses the SNMPv2c `GetBulk` command to gather information from devices in your network environment. If ☐ disabled, NNMi uses the SNMP `Get` or `GetNext` command to gather information from devices in your network environment (requesting responses for one SNMP OID at a time).
SNMP Proxy Address	*Prerequisite*: The NNMi administrator must specify one or more SNMP Proxy Servers in the NNMi Communication Configuration settings. The IP address of the server that is acting as the SNMP Proxy Server for this SNMP agent. Your NNMi administrator might have set up one or more SNMP Proxy Servers to enable communication with nodes that otherwise might be unreachable. For example, when a node to be managed is behind a firewall. The SNMP Proxy Server enables NNMi to manage these nodes in the same way as nodes that provide SNMP access directly.

Basic Attributes, continued

Attribute	Description
SNMP Proxy Port	*Prerequisite:* The NNMi administrator must specify one or more SNMP Proxy Servers in the NNMi Communication Configuration settings. The port number on the server that is acting as the SNMP Proxy Server for this SNMP Agent. See SNMP Proxy Address (previous attribute) for more information.
SNMP 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.

SNMP Agent State Attributes

Attribute	Description
Agent SNMP State	Indicates whether the SNMP agent is available and how NNMi is using SNMP to interact with this SNMP agent. Possible values are: **Normal** – Indicates that the agent responds to requests requiring authentication and login. The following values indicate NNMi could not gather the required data: **No Polling Policy** - No polling policy exists for this monitored attribute. **Not Polled** - 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. **Not Provided** — The device does not support providing information for this monitored attribute. **Not Responding** – Indicates that the SNMP agent does not respond to requests requiring authentication and login. **Unavailable** - The agent responded with a value outside the range of possible values or returned a null value. **Unset** – Currently not used by NNMi. State is determined by the State Poller Service. The current state contributes towards the status calculation for the agent. See "SNMP Agent Form: Status Tab" on page 176 for more information.
Management Address ICMP State	Indicates whether NMi is communicating with the management address. Possible values are: **Responding** – Indicates that the management address is being polled and is responding to an ICMP ping.

SNMP Agent State Attributes, continued

Attribute	Description
	Not Responding – Indicates that the management address is being polled, but is not responding to an ICMP ping. **Not Polled** – 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. The following values indicate NNMi encountered trouble while trying to gather the required data: **No Polling Policy** – No polling policy exists in Monitoring Configuration settings for this monitored attribute. **Unavailable** – Unable to determine the State. For example, the ICMP poll returned a value outside the range of possible values or returned a null value. **Unset** – Currently not used by NNMi. **Note:** NNMi's current Monitoring configuration settings must provide **ICMP Fault Monitoring**: **Enable Management Address Polling** (default or node setting). State is determined by the State Poller Service. The current state contributes towards the status calculation for the SNMP Agent. See the "SNMP Agent Form: Status Tab" on the next page for more information.
Management Address ICMP Response Time	Indicates the State of the ICMP response time between the management server and the selected node. Possible values are: **Nominal** – Indicates the ICMP response time was between 0 and the configured High Value. **Not Polled** – 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. If thresholds are set, the following value is also possible: **High** – Indicates a higher than configured ICMP response time between the management server and the selected node. The following values indicate NNMi encountered trouble while trying to gather the required data: **No Polling Policy** – No polling policy exists in Monitoring Configuration settings for this monitored attribute. **Unavailable** – Unable to determine the State. For example, the ICMP poll returned a value outside the range of possible values or returned a null value.

SNMP Agent State Attributes, continued

Attribute	Description
	Note: NNMi's current Monitoring configuration settings must provide **ICMP Fault Monitoring**: **Enable Management Address Polling** (default or node setting).
Management Address ICMP Response Time Baseline	Indicates the ICMP response time between the management server and the selected node is abnormal based on the computed baseline. Possible values are **Not Polled** – 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. Additional possible values include: Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics) -- click here for more information. **Normal Range** – Indicates State Poller collected values within the normal range when compared to the baseline data collected for the management address response time. If baseline thresholds are set, the following value is also possible: **Abnormal Range** – Indicates State Poller has collected values outside the normal range when compared to the baseline data collected for the management address response time. **Note:** NNMi's current Monitoring configuration settings must provide **ICMP Fault Monitoring**: **Enable Management Address Polling** (default or node setting).
State Last Modified	The date and time of the most recent update of any of the values in the SNMP Agent State attributes (in this table).
Hosted On Node	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). Click the Lookup icon and select Show Analysis or Open to display more information about the node.

SNMP Agent Form: Status Tab

The "SNMP Agent Form" on page 168 provides details about the SNMP Agent of the selected node or interface.

For information about each tab:

Status

Attribute	Description
Status	Overall status for the current SNMP agent. NNMi follows the ISO standard for status classification. Possible values are: No Status Normal Disabled Unknown Warning Minor Major Critical For information about how the current status was determined, see "SNMP Agent Form: Conclusions Tab" below. Status reflects the most serious outstanding conclusion.
Status Last Modified	Date and time indicating when the Status was last set.

Status History Table

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

SNMP Agent Form: Conclusions Tab

The "SNMP Agent Form" on page 168 provides details about the SNMP Agent of the selected node or interface.

For information about each tab:

Outstanding Status Conclusion Values

Attribute	Description
Outstanding Status	The dynamically generated list of summary statuses for the SNMP agent that contributed to the current overall Status of the selected SNMP agent. Status is set by the Causal

Outstanding Status Conclusion Values, continued

Attribute	Description
Conclusions	Engine. Each Conclusion listed is still outstanding and applies to the current overall Status. 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. The Status value is correlated based on the most critical Conclusions. Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion. The following table describes the possible Conclusions that might appear for an SNMP Agent object. **Note:** A **Y** in the **Incident?** column indicates that the Conclusion results in an incident.

Critical Status Conclusions

Conclusion	Description	Status	Incident?
SNMPAgentNotResponding	The SNMP agent is not responding to SNMP queries on the selected node.	Critical	Y

Minor Status Conclusions

Conclusion	Description	Status	Incident?
SNMPAgentPingNotResponding	The address associated with this SNMP Agent is not responding to ping.	Minor	N

Warning Status Conclusions

Conclusion	Description	Status	Incident?
ManagementAddress ICMPResponseTimeAbnormal	Indicates there is an abnormal Internet Control Message Protocol (ICMP) response time from the NNMi management server to the selected node. ICMP messages are typically used for diagnostic or routing purposes for determining whether a host or router could	Warning	Y

Outstanding Status Conclusion Values, continued

Attribute	Description

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

Normal Status Conclusions

Conclusion	Description	Status	Incident?
ManagementAddress ICMPResponseTimeNominal	Indicates that the Internet Control Message Protocol (ICMP) response time from the management server to the selected node is within the threshold range 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
	<table><tr><th>Conclusion</th><th>Description</th><th>Status</th><th>Incident?</th></tr><tr><td>ManagementAddress ICMPResponseTimeNormal</td><td>Indicates I 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.</td><td>Normal</td><td>N</td></tr><tr><td>SNMPAgentPingResponding</td><td>The address associated with this SNMP Agent is responding to ping.</td><td>Normal</td><td>N</td></tr><tr><td>SNMPAgentResponding</td><td>The SNMP Agent is responding to SNMP requests.</td><td>Normal</td><td>N</td></tr></table>

SNMP Agent Form: Incidents Tab

The "SNMP Agent Form" on page 168 provides details about the SNMP Agent of the selected node or interface.

For information about each tab:

Incidents Table

Attribute	Description
Associated Incidents	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. Double-click the row representing an incident. The "Incident Form" on page 437 displays all details about the selected incident.

SNMP Agent Form: Registration Tab

The "SNMP Agent Form" on page 168 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 client and the date and time from the NNMi management server. **Note:** This value does not change when a node is rediscovered. This is because the Node object is modified, but not created.
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. Note the following: • 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. • 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.

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.

Web Agent Form (NNMi Advanced)

The Web Agent form provides details about the **Web Agent**[1] assigned to the currently selected node. This form is useful when you want to view more details about the Web 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 Web Agent.

For information about each tab:

Basic Attributes

Attribute	Description
Name	The type of the Web Agent. For example, VMware vSphere indicates the agent is runs on a VMware ESXi hypervisor.
Hostname	The FQDN hostname of the server. For example, in a VMware environment, the VMware ESXi server's hostname.
Mode	*NNMi administrators only*. Click here for more information.

[1]The Web Agent represents a management service running on a device and contains the settings NNMi uses to communicate with the device.

Basic Attributes, continued

Attribute	Description
	Enables you to specify how NNMi determines the values of the editable Attributes within this instance of the Web Agent form. **Note:** When the node is first discovered, the Web Agent's Mode = **Auto** by default. NNMi discovers and monitors Nodes using the Communication Configuration settings. See Configuring Communication Protocol for more information. **Web Agent Settings Mode Options** **Option** / **Description** **Auto** — NNMi uses the current appropriate Communication Configuration settings to determine the values of the Attributes within this instance of the Web Agent form. See Configuring Communication Protocol for more information. **Locked** — The NNMi Administrator controls the values of the *editable* Attributes within this instance of the Web Agent form for discovery and monitoring. Any future updates to those configuration settings must be established within this instance of the Web Agent form. **Tip:** You can also use nnmcomunication.ovpl to set the Mode and view this Web Agent's configuration settings.
Agent Enabled	Indicates whether the agent is enabled. The Web Agent is enabled when this check box is selected. **Note:** When an agent is Disabled, any data previously reported by that agent is preserved in the NNMi database. Data reported by an Enabled agent is updated as new data is received. *NNMi administrators only*. Click here for more information. To disable the Web Agent, clear the check box.
Scheme	Indicates the mode of communication between NNMi and the Web Agent. Default scheme is HTTPS.
Port	Port configuration for this Web Agent. Default 80.
Timeout	(Seconds:Milliseconds) Time that NNMi waits for a response from the device to a Web Agent query before reissuing the request.
Last Modified	

Basic Attributes, continued

Attribute	Description
Last Modified By	

Web Agent State Attributes

Attribute	Description
Web Agent State	Indicates whether the Web Agent is available and how NNMi is interacting with this Web agent. Possible values are: **Normal** – Indicates that the agent responds to requests requiring authentication and login. The following values indicate NNMi could not gather the required data: **No Polling Policy** - No polling policy exists for this monitored attribute. **Not Polled** - 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. **Not Provided** — The device does not support providing information for this monitored attribute. **Not Responding** – Indicates that the Web Agent does not respond to requests requiring authentication and login. **Unavailable** - The agent responded with a value outside the range of possible values or returned a null value. **Unset** – Currently not used by NNMi. State is determined by the State Poller Service. The current state contributes towards the status calculation for the agent. See "Web Agent Form: Status Tab (NNMi Advanced)" on page 185 for more information.
State Last Modified	The date and time of the most recent update of any of the values in the Web Agent State attributes (in this table).
Hosted On Node	Device on which the Web Agent resides.

Web Agent Form: Device Credentials Tab (NNMi Advanced)

The "Web Agent Form (NNMi Advanced)" on page 181 provides details about the **Web Agent**[1] of the selected node or interface.

For information about each tab:

Device Credentials Attributes

Attribute	Description
User Name	The user name with which NNMi connects to the Web Agent.
Password	Password of the above user.

Web Agent Form: Managed Nodes Tab (NNMi Advanced)

The Managed Node tab lists all the nodes currently managed by the **Web Agent**[2], including the hypervisor that hosts the Web Agent and the virtual machines residing on that hypervisor.

For information about each tab:

Managed Nodes Table

Attribute	Description
Status	Status of the node.
Device Category	Category of the device.
Name	Name of the node.
Hostname	FQDN of the node.
Management Address	IP address of the node.
System Location	Location of the node.
Device Profile	Type of device.
Agent Enabled	Indicates whether a Web Agent is enabled on this node.
Status Last Modified	Last time of update.
Notes	

[1]The Web Agent represents a management service running on a device and contains the settings NNMi uses to communicate with the device.
[2]The Web Agent represents a management service running on a device and contains the settings NNMi uses to communicate with the device.

Web Agent Form: Incidents Tab (NNMi Advanced)

The Web Agent Form: Incidents Tab shows all the open incidents originating from the hypervisor that hosts the **Web Agent**[1].

For information about each tab:

Incidents Table

Attribute	Description
Associated Incidents	Table view of the incidents associated with the selected Web 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 Web Agent. Double-click the row representing an incident. The "Incident Form" on page 437 displays all details about the selected incident.

Web Agent Form: Status Tab (NNMi Advanced)

The "Web Agent Form (NNMi Advanced)" on page 181 provides details about the **Web Agent**[2].

For information about each tab:

Status

Attribute	Description
Status	Overall status for the current Web Agent. NNMi follows the ISO standard for status classification. Possible values are: No Status Normal Disabled Unknown Warning Minor Major Critical For information about how the current status was determined, see "Web Agent Form:

[1]The Web Agent represents a management service running on a device and contains the settings NNMi uses to communicate with the device.
[2]The Web Agent represents a management service running on a device and contains the settings NNMi uses to communicate with the device.

Status, continued

Attribute	Description
	Conclusions Tab (NNMi Advanced)" on the next page. Status reflects the most serious outstanding conclusion.
Status Last Modified	Date and time indicating when the Status was last set.

Status History Table

Attribute	Description
Status History	List of the last 30 changes in the status for the Web Agent. This view is useful for obtaining a summary of the Web Agent 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.

Web Agent Form: Conclusions Tab (NNMi Advanced)

The "Web Agent Form (NNMi Advanced)" on page 181 provides details about the **Web Agent**[1] of the selected node or interface.

For information about each tab:

Outstanding Status Conclusion Values

Attribute	Description
Outstanding Status Conclusions	The dynamically generated list of summary statuses for the Web agent that contributed to the current overall Status of the selected Web agent. Status is set by the Causal Engine. Each Conclusion listed is still outstanding and applies to the current overall Status. This view is useful for obtaining a quick summary of how the Status of Web Agent in the node contributes to the current Status of the Web Agent. The Status value is correlated based on the most critical Conclusions. Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion. The following table describes the possible Conclusions that might appear for an Web Agent object.

[1]The Web Agent represents a management service running on a device and contains the settings NNMi uses to communicate with the device.

Outstanding Status Conclusion Values, continued

Attribute	Description
	Note: A **Y** in the **Incident?** column indicates that the Conclusion results in an incident. **Critical Status Conclusions** **Conclusion** / **Description** / **Status** / **Incident?** WebAgentNotResponding / The Web agent is not responding to web queries requiring authentication and login on the selected node. / Critical / Y **Normal Status Conclusions** **Conclusion** / **Description** / **Status** / **Incident?** WebAgentResponding / The Web Agent is responding to web service requests that require authentication and login. / Normal / N

Web Agent Form: Registration Tab (NNMi Advanced)

The "Web Agent Form (NNMi Advanced)" on page 181 provides details about the **Web Agent**[1] 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 client and the date and time from the NNMi management server. **Note:** This value does not change when a node is rediscovered. This is because the Node object is modified, but not created.
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. Note the following: • 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

[1]The Web Agent represents a management service running on a device and contains the settings NNMi uses to communicate with the device.

Registration Attributes, continued

Attribute	Description
	Completed. • 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.

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.

Web Agent Form: Trusted Certificates Tab (NNMi Advanced)

Note: This tab is for administrators only. The tab does not show any information if you do not log on as an NNMi administrator.

The Web Agent Form: Trusted Certificates tab shows all the trusted certificates that are uploaded to the NNMi management server to facilitate the HTTPS communication between the **Web Agent**[1] and NNMi.

For information about each tab:

Trusted Certificate Attributes

Attribute	Description
Subject DN	The Subject Distinguished Name (Subject DN) of the certificate.
Valid From	The *Valid From* and *Valid To* values together define the validity period of the certificate.
Valid To	

Stored Agent Certificate Form (NNMi Advanced)

Note: This form is for administrators only. You cannot open this form if you do not log on as an NNMi administrator.

The Stored Agent Certificate form shows the following details of the selected trusted certificate that is associated with the Web Agent:

[1]The Web Agent represents a management service running on a device and contains the settings NNMi uses to communicate with the device.

- Subject DN
- Valid From
- Valid To
- CA
- Issuer DN
- UUID
- Serial Number
- Finger Print

Basic Attributes: Stored Agent Certificate

Attribute	Description
Subject DN	The Subject Distinguished Name (Subject DN) of the certificate.
Valid From	The *Valid From* and *Valid To* values together define the validity period of the certificate.
Valid To	
CA	Indicates whether the certificate is issued by a certificate authority.
Issuer DN	Indicates the name of the issuer of the certificate
UUID	Indicates the UUID of the certificate.
Serial Number	Indicates the serial number of the certificate.
Finger Print	Shows the finger print associated with the certificate.

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.

Basic Attributes, continued

Attribute	Description
	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 *other than* Default Tenant can have Layer 2 Connections *only* to devices within the same Tenant or the Default Tenant.
Notes	(*NNMi Advanced - Global Network Management feature*) 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 subnet. Information might include its use; for example, point to point for dialup. You might also use this attribute to track which geographical group might use the subnet. Type a maximum of 1024 characters. Alpha-numeric, spaces, and special characters (~ ! @ # $ % ^ & * ( ) _+ -) are permitted. **Note:** You can sort your subnet table views based on this value. Therefore, you might want to include keywords for this attribute value.

IP Subnet Form: IP Addresses Tab

The "IP Subnet Form" on the previous page provides details about the selected subnet.

For information about each tab:

IP Addresses Table

Attribute	Description
IP Addresses	Table view of the IP addresses associated with the selected subnet. You can use this table to determine the state, address, and interface, and parent node for each address associated with the selected subnet. Double-click the row representing an IP address. The "IP Address Form" on page 160 displays all details about the selected IP address.

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. **Note:** This value does not change when a node is rediscovered. This is because the Node object is modified, but not created.
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. Note the following: • 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. • 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.

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 connections are determined by a common VLAN Id. The *name* assigned to that

Basic Attributes, continued

Attribute	Description
VLAN Name	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): Global VLAN Name = NNMi uses the lowest sort-order name from all available names designated by member Nodes. **Tip:** If you see an attribute named *Local VLAN Name* = the VLAN name assigned by the configuration settings on the currently selected Node\Interface.
VLAN Id	The identification value for the current VLAN. This value is taken directly from the MIB file provided by the Vendor.

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

VLAN Statistics Attributes

Attribute	Description
Member Node [Interface]	`hostname[Interface Name]` 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. NNMi selects the Member Node using the following criteria: • The node is a member of the VLAN. • The node has the lexicographically ordered first node hostname. • The User Group to Security Group mapping enables the user to view the node. NNMi selects the Member Interface using the following criteria: • The interface must be on the Member Node. • The interface is a member of the VLAN. • The interface has the lexicographically ordered first interface name. • The User Group to Security Group mapping enables the user to view the node to which the interface belongs.
Member Node Count	Specifies the number of nodes that belong to the current VLAN.

Related Topics:

"VLANs View (Inventory)" on page 44

VLAN Form: Ports Tab

Note: A trunk port can participate in multiple VLANs.

The "VLAN Form" on page 191 provides details about the selected VLAN.

For information about each tab:

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 229 displays all details about the selected Port.

Related Topics:

"VLANs View (Inventory)" on page 44

Chassis Form

The Chassis form provides details about the Chassis you selected on the Node form or Inventory: "Chassis View" on page 45. The following table describes the fields included on Basics section of the Chassis form.

For information about each tab:

Basic Attributes

Attribute	Description
Name	The name of the chassis. Sometimes it's the descriptive string used by the network administrator to name the chassis. For example, C2950T, H3C S7503E, and Unit #2 S9505E. If the Name value is null, NNMi uses the Component Identifier value (see "Chassis Form: General Tab" on page 199).
Type	The type of Physical Component for this object: Chassis.
Managed By	The node using this chassis or the node assigned to the Agent that is managing this chassis. This is the current value in NNMi's database for the Name attribute of the host 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). Click the Lookup icon and select Show Analysis or Open to display more information about the node.
Status	Overall status for the current chassis. NNMi follows the ISO standard for status

Basic Attributes, continued

Attribute	Description
	classification. See the "Chassis Form: Status Tab" on page 206 for more information. Possible values are: Normal Warning Minor Major Critical Unknown No Status Chassis status is derived from polling results for Administrative State, Operational State, and the most serious outstanding conclusion. See the "Chassis Form: Conclusions Tab" on page 208 for information about how the current status was determined. See "Watch Status Colors" on page 406 for more information about possible status values. **Note:** The icons are displayed only in table views.
Management Mode	The *calculated* Management Mode for the chassis according to the Management Mode Hierarchy. This value reflects the current management mode of this chassis's parent object (either the Parent Component chassis or the Managed By node). See "How NNMi Assigns the Management Mode to an Object" on page 591. (*NNMi Advanced - Global Network Management feature*) 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. **Note:** If the NNMi Security configuration permits, you can change this setting using **Actions** → **Management Mode**. **Tip:** You can also right-click any object in a table or map view to access the items available within the **Actions** menu.
Direct Management Mode	Indicates whether or not NNMi is currently monitoring the chassis. Possible values are: **Inherited** – Used to indicate that the chassis should inherit the Management Mode from the chassis's parent object (either the Parent Component chassis or the Managed By node). **Not Managed** – Used to indicate that NNMi does not discover or monitor the chassis. **Out of Service** – Used to indicate the chassis is unavailable because it is out of service

Basic Attributes, continued

Attribute	Description
	or participating in a Scheduled Node Outage. NNMi does not discover or monitor this Chassis. NNMi administrators and Level 2 Operators can use the drop-down selection list to change the current setting. **Note:** If you change the Direct Management Mode using **Actions → Management Mode**, NNMi updates the calculated Management Mode on the form. If you manually set the Direct Management Mode and then Save your changes, the Management Mode value is not updated until you refresh the form.
Parent Component	If this chassis is plugged into another chassis, the Name of that chassis is listed here.
Redundancy Group	Indicates whether this chassis participates in a group of chassis that provide redundancy protection against chassis failure.

Physical Component State Attributes

Attribute	Description
Administrative State	Either the current chassis 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 chassis. See the "Chassis Form: Status Tab" on page 206 for more information. **Note:** If the chassis's SNMP agent supports only the Internet Engineering Task Force (IETF) ENTITY-MIB, no state or status information is available. NNMi sets this state to **No Polling Policy** and the chassis status to No Status. If you look on the parent "Node Form" on page 65, you will see the `com.hp.nnm.capability.card.ietf.entity` capability in the list. Possible values are: **Up** – The SNMP agent responded with a chassis administrative status value of Up. **Down** – The SNMP agent responded with a chassis administrative status value of Down. **Other** – The SNMP agent responded with a value for chassis administrative status that is not recognized. The following values indicate NNMi could not gather the required data: **Agent Error** – Indicates an error was returned in response to the query. **No Polling Policy** - No polling policy exists for this monitored attribute.

Physical Component State Attributes, continued

Attribute	Description
	Not Polled - 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. **Not Provided** — The device does not support providing information for this monitored attribute. **Unavailable** - The agent responded with a value outside the range of possible values or returned a null value. **Unset** – Currently not used by NNMi.
Operational State	The current chassis 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 chassis. See the "Chassis Form: Status Tab" on page 206 for more information. **Note:** If the chassis's SNMP agent supports only the Internet Engineering Task Force (IETF) ENTITY-MIB, no state or status information is available. NNMi sets this state to **No Polling Policy** and the chassis status to No Status. If you look on the parent "Node Form" on page 65, you will see the `com.hp.nnm.capability.card.ietf.entity` capability in the list. Possible values are: **Up** – The SNMP agent responded that the chassis is operationally up, ready to receive and send network traffic. **Disabled** – The chassis's *Administrative State* is set to **Down**. **Down** – The SNMP agent responded that the chassis is operationally down. **Dormant** – Indicates the chassis is in a "pending" state, waiting for some external event. **Minor Fault** – Indicates that the chassis or one of its hardware components is experiencing a partial failure. **Not Present** – Indicates that the chassis module is not installed or is missing. **Other** – The SNMP agent responded with a value for chassis operational status that is not recognized. **Testing** – The SNMP agent responded that the chassis is in test mode. **Transient** – Indicates the chassis is in a transient state. For example, rebooting. **Unknown** – The SNMP agent responded with a chassis operational status value of

Physical Component State Attributes, continued

Attribute	Description
	unknown. The following values indicate NNMi could not gather the required data: **Agent Error** – Indicates an SNMP error was returned in response to an SNMP query to this agent. **No Polling Policy** - No polling policy exists in Monitoring Configuration settings for this monitored attribute. **Not Polled** - 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 **Unavailable** - The SNMP agent responded with a value for chassis operational status of *Not-Specified*, 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. **Unset** – Currently not used by NNMi.
Standby State	Either the current MIB-II *Standby State* 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 chassis. See the "Chassis Form: Status Tab" on page 206 for more information. **Note:** If the chassis's SNMP agent supports only the Internet Engineering Task Force (IETF) ENTITY-MIB, no state or status information is available. NNMi sets this state to **No Polling Policy** and the chassis status to No Status. If you look on the parent "Node Form" on page 65, you will see the `com.hp.nnm.capability.card.ietf.entity` capability in the list. Possible values are: **Active** - Indicates the chassis is the active chassis in the Chassis Redundancy Group. **Cold-Standby** - Indicates the chassis is not in use, but is available to take over the role of the active chassis after it is initialized. **Hot-Standby** - Indicates the chassis is not in use, but can immediately take over the role of the active chassis. **Standby** - Indicates the chassis is a candidate to become the next active chassis. **Error** - Indicates the chassis cannot take over the role of active or standby chassis in the Chassis Redundancy Group. **Other** – The SNMP agent on the chassis responded with a value for Standby State of

Physical Component State Attributes, continued

Attribute	Description
	Other or one that is not recognized. **Transient** – Indicates the chassis is in a transient state. For example, rebooting. **Unknown** - Indicates the chassis is unable to report Standby State. The following values indicate NNMi could not gather the required data: **Agent Error** – Indicates an error was returned in response to the query. **No Polling Policy** - No polling policy exists for this monitored attribute. **Not Polled** - 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. **Not Provided** — The device does not support providing information for this monitored attribute. **Unavailable** - The agent responded with a value outside the range of possible values or returned a null value. **Unset** – Currently not used by NNMi.
Previous Standby State	The Standby State that was determined before the current Standby State. See Standby State 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	Provided for network operators to use for any additional information about this chassis that you want to communicate to your team. Type a maximum of 1024 characters. Alpha-numeric, spaces, and special characters (~ ! @ # $ % ^ & * ( ) _+ -) are permitted. **Note:** You can sort your Chassis table views based on this value. Therefore, you might want to include keywords for this attribute value. (*NNMi Advanced - Global Network Management feature*) 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.

Chassis Form: General Tab

The "Chassis Form" on page 193 provides details about the selected chassis.

For information about each tab:

General Attributes

Attribute	Description
Model Name	Chassis model name or number designator, determined by the vendor.
Model Type	The hardware manufacture's designator for the Chassis, determined by the vendor. For example: • cevChassisCat2950t24 • hpSwitchJ8692A • hpSwitch1600
Serial Number	Chassis serial number, determined by the vendor.
Firmware Version	The firmware version or revision for the Chassis, determined by the vendor. For example,12.1(22)EA11.
Hardware Version	The hardware version or revision for the Chassis, determined by the vendor. For example, VER.B.
Software Version	The software version or revision for the Chassis, determined by the vendor. For example, 12.1(22)EA11.
Component Identifier	The unique value assigned to each Physical Component: Chassis. The value chosen is always consistent with the Name value assigned to the Chassis's hosted port. If ENTITY-MIB is the *only MIB* supported for a particular Chassis, this attribute has the same value as the Physical Index attribute.
Physical Index	NNMi gathers this attribute value if the ENTITY-MIB is supported by the chassis's vendor.
Description	The description assigned to the Chassis by the operating system of the device in which the Chassis is mounted. Examples: • Cisco Catalyst c2950 switch with 24 10/100 BaseTX ports and 2 10/100/1000 BaseT ports • ProCurve J8692A Switch 3500yl-24G • HPE J4120A ProCurve Switch 1600M

Chassis Form: Ports Tab

The "Chassis Form" on page 193 provides details about the selected chassis.

For information about each tab:

Ports Associated with this Chassis

Attribute	Description
Ports	Table of all of the ports associated with the selected chassis. Use this table to access information about each port associated with the selected chassis. Double-click the row representing a Port. The "Port Form" on page 229 displays all details about the selected Port.

Chassis Form: Child Components Tab

The "Chassis Form" on page 193 provides details about the selected chassis.

For information about each tab:

Child Components Attached to this Chassis

Attribute	Description
Child Components	Table of all of the Physical Components of type Card or Chassis that are plugged into the selected chassis. Use this table to access information about each child card or child chassis associated with the selected parent chassis. Double-click the row representing a child Physical Component. The "Chassis Form" on page 193 or "Card Form" on page 211 displays all details about the selected card or chassis.

Chassis Form: Hosted Nodes Tab

(*NNMi Advanced*) The Chassis Form: Hosted Nodes tab appears if the Chassis is hosting nodes other than the node that is managing this Chassis (the Node identified in this Chassis's Managed By attribute). For example, a virtual device.

For information about each tab:

Hosted Nodes Table

Attribute	Description
Status	See the Status information in "Node Form" on page 65.
Device Category	The NNMi administrator specifies this attribute value. See Configure Device Category Icons.
Name	See the Name information in "Node Form" on page 65.
Hostname	See the Hostname information in "Node Form" on page 65.
Management Address	See the Management Address information in "Node Form" on page 65.
System Location	See the System Location information in "Node Form: General Tab" on page 73.

Hosted Nodes Table, continued

Attribute	Description
Device Profile	See the Device Profile information in "Node Form" on page 65.
SNMP Agent Enabled	See the SNMP Agent Enabled information in "Node Form" on page 65.
Status Last Modified	See the Status Last Modified information in "Node Form: Status Tab" on page 93.
Notes	See the Notes information in "Node Form" on page 65.

Chassis Form: Capabilities Tab

The "Chassis Form" on page 193 provides details about the selected chassis.

The Chassis Form: Capabilities tab displays a table of any capabilities added to the chassis object by NNMi or an external application. Capabilities enable NNMi and application programmers to provide more information about a chassis 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 Chassis

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

Chassis Capabilities Provided by NNMi

The "Chassis Form: Capabilities Tab" above displays a table of any capabilities added to a particular chassis object. Capabilities enable NNMi and application programmers to provide more information about a chassis 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*> = chassis, card, ipaddr (address), iface (interface), lag (**Link Aggregation**[1] or **Split Link Aggregation**[2] interface), node, rrp (Router Redundancy), or metric (Node Sensor or Physical Sensor).

<*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.

Chassis Capability Attribute Values

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

Physical Component Capability Form (Chassis)

This form describes a capability added to the Physical Component object by NNMi or an external application. Capabilities enable NNMi and application programmers to provide more information about a Physical Component 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.

Physical Component Capability Attributes

Attribute	Description
Capability	Label used to identify the Capability that was added to the Physical Component object. For more information see the following: • "Chassis Form: Capabilities Tab" on the previous page shows a list of all available Capabilities for that chassis.
Unique Key	Used as a unique identifier for the Capability. Any capability provided by NNMi begins with the prefix `com.hp.nnm.capability`. For more information: • "Chassis Capabilities Provided by NNMi" on the previous page

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

Chassis Form: Custom Attributes Tab

The Chassis Form: Custom Attributes tab displays a table view of any Custom Attributes that have been added to the selected chassis. Custom Attributes provide additional information about an object instance.

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 can be replicated from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager configure which Regional Custom Attributes they want (Global Manager: Configure Custom Attribute Replication). NNMi administrators can also configure Custom Attribute values that are unique to the Global Manager's environment (Customize Object Attributes).

Custom Attributes Table

Attribute	Description
Name	Name that identifies this Custom Attribute. This name appears in the table view on the Custom Attributes tab in Chassis forms. Limit 50 of any combination of keyboard entries including spaces.
Value	The actual value for the Custom Attribute for the selected chassis. Limit 2,000 of any combination of keyboard entries including spaces. For more information, see "Physical Component Custom Attribute Form (Chassis)" below.

Physical Component Custom Attribute Form (Chassis)

Physical Component Custom Attributes provide additional information about a Chassis object instance. NNMi Administrators or applications that have been integrated with NNMi can create these Custom Attributes.

The required settings for these attributes are described in the table below.

(*NNMi Advanced - Global Network Management feature*) Custom Attribute values can be replicated from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager configure which Regional Custom Attributes they want (Global Manager: Configure Custom Attribute Replication). NNMi administrators can also configure Custom Attribute values that are unique to the Global Manager's environment (Customize Object Attributes).

Basics Attributes

Attribute	Description
Name	Name that identifies this Custom Attribute. The name appears in the table view on the Custom Attributes tab in the Chassis form. Limit 50 of any combination of keyboard entries including spaces.

Basics Attributes, continued

Attribute	Description
Value	Value assigned to this Custom Attribute for the selected Chassis object. Limit 2,000 of any combination of keyboard entries including spaces. For more information, see "Chassis Form: Custom Attributes Tab" on the previous page.

Chassis Form: Physical Sensors Tab

The "Chassis Form" on page 193 provides details about the selected chassis.

For information about each tab:

The Chassis Form: Physical Sensors tab displays a table of any Physical Sensors associated with the chassis object for fault monitoring:

- Fan
- Power Supply
- Temperature
- Voltage

(*NNM iSPI Performance for Metrics*) If the HPE Network Node Manager iSPI Performance for Metrics Software is installed and configured within your environment, the table can also include Physical Sensors associated with the chassis object for performance monitoring and thresholds (click here for more information):

- Backplane Utilization

  Threshold based on the percentage of backplane usage compared to the total amount of available backplane resources.

Tip: See "Physical Sensor Form" on page 244 for more details about the node sensor attributes that appear in this view's column headings. Node Sensors are displayed in three views: "Physical Sensors View" on page 47, "Non-Normal Physical Sensors View" on page 394, and "Unmanaged Physical Sensors View" on page 585.

Physical Sensors Associated with this Chassis

Attribute	Description
Physical Sensors	Table view of the fault and performance metrics associated with the current chassis. You can use this table to determine the Status, Name, and Type for each Physical Sensor metric associated with the selected chassis. Double-click the row representing a Physical Sensor. The "Physical Sensor Monitored Attribute Form" on page 247 displays all details about the selected Physical Sensor. **Note:** The NNMi administrator can set Physical Sensor thresholds. For more information, see "Chassis Form: Physical Sensors Tab" above and "Card Form: Physical Sensors Tab" on page 222.

Chassis Form: Node Sensors Tab

The "Chassis Form" on page 193 provides details about the selected chassis.

For information about each tab:

The Chassis Form: Node Sensors tab displays a table of any Node Sensors associated with the chassis object for fault monitoring. Each Node Sensor identifies the health aspect that is being monitored.

(*NNM iSPI Performance for Metrics*) If the HPE Network Node Manager iSPI Performance for Metrics Software is installed and configured within your environment, the table can include Node Sensors associated with the chassis object for performance monitoring and thresholds (click here for more information):

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

Tip: See "Node Sensor Form" on page 232 for more details about the node sensor attributes that appear in this view's column headings. Node Sensors are displayed in three views: "Node Sensors View" on page 47, "Non-Normal Node Sensors View" on page 393, and "Unmanaged Node Sensors View" on page 585.

Node Sensors Associated with this Chassis

Attribute	Description
Node Sensors	Table view of the fault and performance metrics associated with the current chassis. You can use this table to determine the Status, Name, and Type for each Node Sensor metric associated with the selected chassis. Double-click the row representing a Node Sensor. The "Node Sensor Form" on page 232 displays all details about the selected Node Sensor. **Note:** The NNMi administrator can set Node Sensor thresholds. For more information, see "Node Form: Node Sensors Tab" on page 84, "Chassis Form: Node Sensors Tab" above, and "Card Form: Node Sensors Tab" on page 223.

Chassis Form: Incidents Tab

The "Chassis Form" on page 193 provides details about the selected chassis.

For information about each tab:

Incidents Associated with this Chassis

Attribute	Description
Incidents	Table of the Incidents associated with the selected chassis. 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 chassis. Double-click the row representing an incident. The "Incident Form" on page 437 displays all details about the selected incident. **Note:** See "Incident Form" on page 437 for more details about the incident attributes that appear in the incident table's column headings.

Chassis Form: Status Tab

The "Chassis Form" on page 193 provides details about the selected chassis.

For information about each tab:

Overall Status Attributes

Attribute	Description
Status	Overall status for the current chassis. NNMi follows the ISO standard for status classification. Possible values are: **No Status**: The chassis and all of its cards are not polled. **Normal**: The Operational State of the Chassis Up. The Operational State of all cards in the chassis is Up. **Unknown**: The SNMP Agent associated with the Chassis does not respond to SNMP queries. **Warning**: The Operational State of the Chassis not Down. The Operational State of one card in the chassis is Down. **Minor**: The Operational State of the Chassis not Down. The Operational State of some (but not all) cards in the chassis is Down. **Major**: The Operational State of the Chassis not Down. The Operational State of *all* cards in the chassis is Down. **Critical**: The Operational State of the Chassis Down. See "Watch Status Colors" on page 406 for more information about possible status values. Physical Component status is derived from SNMP polling results for Administrative State, Operational State, and the most serious outstanding conclusion. For information about how the current status was determined, see the following: • "Card Form: Conclusions Tab" on page 226

Overall Status Attributes, continued

Attribute	Description
	• "Chassis Form: Conclusions Tab" on the next page **Note:** The icons are displayed only in table views.
Status Last Modified	Date and time indicating when the Status was last set.

Physical Component Status History Table

Attribute	Description
Status History	Table of up to the last 30 changes in the status for the Chassis. This table is useful for obtaining a summary of the Chassis Status so that you can better determine any patterns in behavior and activity. Double-click the row representing a Status History. The "Physical Component Status History Form (Card)" on page 225 displays all details about the selected Status.

Physical Component Status History Form (Chassis)

Status is derived from SNMP polling results for Administrative State, Operational State, and the most serious outstanding conclusion.

See the object's conclusions for information about how the current status was determined:

- "Chassis Form: Conclusions Tab" on the next page

Status Attributes

Attribute	Description
Status	Overall status for the current chassis. See "Watch Status Colors" on page 406 for more information about possible status values. NNMi follows the ISO standard for status classification. Possible values are: No Status Normal Disabled Unknown Warning Minor Major

Status Attributes, continued

Attribute	Description
	Critical Physical Component status is derived from SNMP polling results for Administrative State, Operational State, and the most serious outstanding conclusion. **Note:** The icons are displayed only in table views. For more information see the following: • "Chassis Form: Status Tab" on page 206
Status Last Modified	Date and time indicating when the status was last set.

Chassis Form: Conclusions Tab

The "Chassis Form" on page 193 provides details about the selected chassis.

For information about each tab:

Outstanding Status Conclusion Values

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

[1]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

Conclusion	Description	Status	Incident?
ChassisDown	The Operational State of the selected chassis is Down.	Critical	Y

Disabled Status Conclusions

Conclusion	Description	Status	Incident?
ChassisDisabled	SNMP agent reports that the Administrative State for the selected chassis is Down.	Minor	Y

Major Status Conclusions

If any of the following Major chassis conclusions occur, NNMi propagates a major `ChassisMajorInNode` Status Conclusion to the parent Node Form: Conclusions Tab unless the NNMi administrator intentionally disables the propagation using java properties settings.

Conclusion	Description	Status	Incident?
AllCardsDownInChassis	All cards in a chassis are Down.	Major	Y
CardMajorInChassis	One or more cards in a chassis have a status of major.	Major	Y
ChassisWithBadBackplane	One or more backplanes have one or more monitored attributes that are outside the currently configured threshold range.	Major	N
ChassisWithBadFan	One or more fans are out of range or malfunctioning.	Major	N
ChassisWithBadPowerSupply	One or more power supplies are out of range or malfunctioning.	Major	N
ChassisWithBadTemperature	One or more temperature sensors are out of range or malfunctioning.	Major	N
ChassisWithBadVoltage	One or more voltage sensors are out of range or malfunctioning.	Major	N

Minor Status Conclusions

Conclusion	Description	Status	Incident?
CardsDownInChassis	More than one card in a chassis is Down, but not all cards are Down.	Minor	Y

Outstanding Status Conclusion Values, continued

Attribute	Description
	Warning Status Conclusions **Conclusion** / **Description** / **Status** / **Incident?** CardDownInChassis / One card in a chassis is Down, but not all cards are Down. / Normal / N **Unknown Status Conclusions** **Conclusion** / **Description** / **Status** / **Incident?** ChassisUnmanageable / The SNMP agent of the managing Node is not responding. / Unknown / N **Normal Status Conclusions** **Conclusion** / **Description** / **Status** / **Incident?** ChassisUp / The Operational State for the current chassis is Up. / Normal / N CardsUpInChassis / The SNMP agent has determined that all Cards are Up. / Normal / Y

Physical Component Status Conclusions Form (Chassis)

The current Conclusion contributes towards the current overall Status of the selected Physical Component.

Basics Attributes

Attribute	Description
Status	Status is derived from the most serious outstanding Conclusion and SNMP polling results for Administrative State and Operational State.
Time Stamp	The time of the last change in Status.
Conclusion	For more information about each conclusion, see the following: • "Chassis Form: Conclusions Tab" on page 208

Chassis Form: Registration Tab

The "Chassis Form" on page 193 provides details about the selected chassis.

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. **Note:** This value does not change when a node is rediscovered. This is because the Node object is modified, but not created.
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. Note the following: • 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. • 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.

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 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, RSM-Mod, and ATM-OC3-Phy. If the Name value is null, NNMi uses the Component Identifier value (see "Card Form: General Tab" on page 217).
Type	The type of Physical Component for this object: Card.
Managed By	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).

Basic Attributes, continued

Attribute	Description
	Click the Lookup icon and select Show Analysis or Open to display more information about the node.
Status	Overall status for the current card. NNMi follows the ISO standard for status classification. See the "Card Form: Status Tab" on page 224 for more information. Possible values are: Normal Warning Minor Major Critical Disabled Unknown No Status 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 page 226 for information about how the current status was determined. See "Watch Status Colors" on page 406 for more information about possible status values. **Note:** The icons are displayed only in table views.
Management Mode	The *calculated* Management Mode for the card according to the Management Mode Hierarchy. This value reflects the current management mode of this card's parent object (either the Parent Component card or chassis, or the Managed By node). See "How NNMi Assigns the Management Mode to an Object" on page 591. (*NNMi Advanced - Global Network Management feature*) 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. **Note:** If the NNMi Security configuration permits, you can change this setting using **Actions** → **Management Mode**. **Tip:** You can also right-click any object in a table or map view to access the items available within the **Actions** menu.
Direct Management Mode	Indicates whether or not NNMi is currently monitoring the card. Possible values are: **Inherited** – Used to indicate that the card should inherit the Management Mode from this

Basic Attributes, continued

Attribute	Description
	card's parent object (either the Parent Component card or chassis, or the Managed By node). **Not Managed** – Used to indicate that NNMi does not discover or monitor the card. **Out of Service** – Used to indicate the card is unavailable because it is out of service or participating in a Scheduled Node Outage. NNMi does not discover or monitor this card. NNMi administrators and Level 2 Operators can use the drop-down selection list to change the current setting. **Note:** If you change the Direct Management Mode using **Actions → Management Mode**, NNMi updates the calculated Management Mode on the form. If you manually set the Direct Management Mode and then Save your changes, the Management Mode value is not updated until you refresh the form.
Parent Component	If this card is plugged into a chassis or another card, the Name of that chassis or card is listed here.
Redundancy Group	Indicates whether this card participates in a group of cards that provide redundancy protection against card failure.

Physical Component State Attributes

Attribute	Description
Administrative State	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 "Card Form: Status Tab" on page 224 for more information. **Note:** If the card's SNMP agent supports only the Internet Engineering Task Force (IETF) ENTITY-MIB, no state or status information is available. NNMi sets this state to **No Polling Policy** and the card status to No Status. If you look on the parent "Node Form" on page 65, you will see the `com.hp.nnm.capability.card.ietf.entity` capability in the list. Possible values are: **Up** – The SNMP agent responded with a card administrative status value of Up. **Down** – The SNMP agent responded with a card administrative status value of Down. **Other** – The SNMP agent responded with a value for card administrative status that is not recognized.

Physical Component State Attributes, continued

Attribute	Description
	The following values indicate NNMi could not gather the required data: **Agent Error** – Indicates an error was returned in response to the query. **No Polling Policy** - No polling policy exists for this monitored attribute. **Not Polled** - 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. **Not Provided** — The device does not support providing information for this monitored attribute. **Unavailable** - The agent responded with a value outside the range of possible values or returned a null value. **Unset** – Currently not used by NNMi.
Operational State	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 "Card Form: Status Tab" on page 224 for more information. **Note:** If the card's SNMP agent supports only the Internet Engineering Task Force (IETF) ENTITY-MIB, no state or status information is available. NNMi sets this state to **No Polling Policy** and the card status to No Status. If you look on the parent "Node Form" on page 65, you will see the `com.hp.nnm.capability.card.ietf.entity` capability in the list. Possible values are: **Up** – The SNMP agent responded that the card is operationally up, ready to receive and send network traffic. **Disabled** – The card's *Administrative State* is set to **Down**. **Down** – The SNMP agent responded that the card is operationally down. **Dormant** – Indicates the card is in a "pending" state, waiting for some external event. **Minor Fault** – Indicates that the card or one of its hardware components is experiencing a partial failure. **Not Present** – Indicates that the card module is not installed or is missing. **Other** – The SNMP agent responded with a value for card operational status that is not recognized.

Physical Component State Attributes, continued

Attribute	Description
	Testing – The SNMP agent responded that the card is in test mode. **Transient** – Indicates the card is in a transient state. For example, rebooting. **Unknown** – The SNMP agent responded with a card operational status value of *unknown*. The following values indicate NNMi could not gather the required data: **Agent Error** – Indicates an SNMP error was returned in response to an SNMP query to this agent. **No Polling Policy** - No polling policy exists in Monitoring Configuration settings for this monitored attribute. **Not Polled** - 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 **Unavailable** - The SNMP agent responded with a value for card operational status of *Not-Specified*, 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. **Unset** – Currently not used by NNMi.
Standby State	Either the current MIB-II *Standby State* 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 "Card Form: Status Tab" on page 224 for more information. **Note:** If the card's SNMP agent supports only the Internet Engineering Task Force (IETF) ENTITY-MIB, no state or status information is available. NNMi sets this state to **No Polling Policy** and the card status to No Status. If you look on the parent "Node Form" on page 65, you will see the `com.hp.nnm.capability.card.ietf.entity` capability in the list. Possible values are: **Active** - Indicates the card is the active card in the Card Redundancy Group. **Cold-Standby** - Indicates the card is not in use, but is available to take over the role of the active card after it is initialized. **Hot-Standby** - Indicates the card is not in use, but can immediately take over the role of the active card. **Standby** - Indicates the card is a candidate to become the next active card.

Physical Component State Attributes, continued

Attribute	Description
	Error - Indicates the card cannot take over the role of active or standby card in the Card Redundancy Group. **Other** – The SNMP agent on the card responded with a value for Standby State of **Other** or one that is not recognized. **Transient** – Indicates the card is in a transient state. For example, rebooting. **Unknown** - Indicates the card is unable to report Standby State. The following values indicate NNMi could not gather the required data: **Agent Error** – Indicates an error was returned in response to the query. **No Polling Policy** - No polling policy exists for this monitored attribute. **Not Polled** - 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. **Not Provided** — The device does not support providing information for this monitored attribute. **Unavailable** - The agent responded with a value outside the range of possible values or returned a null value. **Unset** – Currently not used by NNMi.
Previous Standby State	The Standby State that was determined before the current Standby State. See Standby State 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	(*NNMi Advanced - Global Network Management feature*) 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 information about this card that you want to communicate to your team. Type a maximum of 1024 characters. Alpha-numeric, spaces, and special characters (~ ! @ # $ % ^ & * ( ) _+ -) are permitted. **Note:** You can sort your Card table views based on this value. Therefore, you might want to include keywords for this attribute value.

Card Form: General Tab

The "Card Form" on page 211 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.
Model Type	The hardware manufacturer's designator for the card, determined by the vendor. For example: • cevCat6kWsSup720Base • wssup720base(1002) • cat6k-ws-sup720-base
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.
Software Version	The software version or revision for the card, determined by the vendor. For example, 12.2 (33)SXI
Component Identifier	The unique value assigned to each Physical Component (card or chassis). The value chosen is always consistent with the Name value assigned to the card's hosted port. For example, the physical index of card hosting port Fa5/1 is 5 and the physical index of card hosting port J8 is J. If ENTITY-MIB is the *only MIB* supported for a particular card, this attribute has the same value as the Physical Index attribute.
Physical Index	NNMi gathers this attribute value if the ENTITY-MIB is supported by the card's vendor.
Description	The description assigned to the card by the operating system of the device in which the card is mounted. Examples: • WS-X5530 1000BaseSXSupervisor Rev. 1.8 • WS-X5225R 10/100BaseTX Ethernet Rev. 1.1 • HP J4111A 8-port 10/100Base-TX module

Card Form: Ports Tab

The "Card Form" on page 211 provides details about the selected card.

For information about each tab:

Ports Associated with this Card

Attribute	Description
Ports	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. Double-click the row representing a Port. The "Port Form" on page 229 displays all details about the selected Port.

Card Form: Child Components Tab

The "Card Form" on page 211 provides details about the selected card.

For information about each tab:

Child Components Attached to this Card

Attribute	Description
Child Components	Table of all of the Physical Component: Cards that are plugged into the selected card. Use this table to access information about each child card associated with the selected parent card. Double-click the row representing a child Physical Component. The "Card Form" on page 211 displays all details about the selected card.

Card Form: Hosted Nodes Tab

(*NNMi Advanced*) The Card Form: Hosted Nodes tab appears if the Card is hosting nodes other than the node that is managing this Card (the Node identified in this Card's Managed By attribute). For example, a virtual device.

For information about each tab:

Hosted Nodes Table

Attribute	Description
Status	See the Status information in "Node Form" on page 65.
Device Category	The NNMi administrator specifies this attribute value. See Configure Device Category Icons.
Name	See the Name information in "Node Form" on page 65.

Hosted Nodes Table, continued

Attribute	Description
Hostname	See the Hostname information in "Node Form" on page 65.
Management Address	See the Management Address information in "Node Form" on page 65.
System Location	See the System Location information in "Node Form: General Tab" on page 73.
Device Profile	See the Device Profile information in "Node Form" on page 65.
SNMP Agent Enabled	See the SNMP Agent Enabled information in "Node Form" on page 65.
Status Last Modified	See the Status Last Modified information in "Node Form: Status Tab" on page 93.
Notes	See the Notes information in "Node Form" on page 65.

Card Form: Capabilities Tab

The "Card Form" on page 211 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.
Unique Key	Double-click the row representing a Capability. The Physical Component Capability Form 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>` = chassis, card, ipaddr (address), iface (interface), lag (**Link Aggregation**[1] or **Split Link Aggregation**[2] interface), node, rrp (Router Redundancy), or metric (Node Sensor or Physical Sensor).

`<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).

Physical Component Capability Form (Card)

This form describes a capability added to the Physical Component object by NNMi or an external application. Capabilities enable NNMi and application programmers to provide more information about a Physical Component 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.

Physical Component Capability Attributes

Attribute	Description
Capability	Label used to identify the Capability that was added to the Physical Component object. For more information see the following: • "Card Form: Capabilities Tab" on the previous page shows a list of all available Capabilities for that cards.

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

Physical Component Capability Attributes, continued

Attribute	Description
Unique Key	Used as a unique identifier for the Capability. Any capability provided by NNMi begins with the prefix `com.hp.nnm.capability`. For more information: • "Card Capabilities Provided by NNMi" on page 219

Card Form: Custom Attributes Tab

The Card Form: Custom Attributes tab displays a table view of any Custom Attributes that have been added to the selected card. Custom Attributes provide additional information about an object instance.

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 can be replicated from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager configure which Regional Custom Attributes they want (Global Manager: Configure Custom Attribute Replication). NNMi administrators can also configure Custom Attribute values that are unique to the Global Manager's environment (Customize Object Attributes).

Custom Attributes Table

Attribute	Description
Name	Name that identifies this Custom Attribute. This name appears in the table view on the Custom Attributes tab in Card forms. Limit 50 of any combination of keyboard entries including spaces.
Value	The actual value for the Custom Attribute for the selected card. Limit 2,000 of any combination of keyboard entries including spaces. For more information, see "Physical Component Custom Attribute Form (Card)" below.

Physical Component Custom Attribute Form (Card)

Physical Component Custom Attributes provide additional information about a Card object instance. NNMi Administrators or applications that have been integrated with NNMi can create these Custom Attributes.

The required settings for these attributes are described in the table below.

(*NNMi Advanced - Global Network Management feature*) Custom Attribute values can be replicated from a Regional Manager (NNMi management server) to the Global Manager. NNMi administrators for the Global Manager configure which Regional Custom Attributes they want (Global Manager: Configure Custom Attribute Replication). NNMi administrators can also configure Custom Attribute values that are unique to the Global Manager's environment (Customize Object Attributes).

Basics Attributes

Attribute	Description
Name	Name that identifies this Custom Attribute. The name appears in the table view on the Custom Attributes tab in the Card form. Limit 50 of any combination of keyboard entries including spaces.
Value	Value assigned to this Custom Attribute for the selected Card object. Limit 2,000 of any combination of keyboard entries including spaces. For more information, see "Card Form: Custom Attributes Tab" on the previous page.

Card Form: Physical Sensors Tab

The "Card Form" on page 211 provides details about the selected card.

For information about each tab:

The Card Form: Physical Sensors tab displays a table of any Physical Sensors associated with the card for fault monitoring:

- Fan
- Power Supply
- Temperature
- Voltage

(*NNM iSPI Performance for Metrics*) If the HPE Network Node Manager iSPI Performance for Metrics Software is installed and configured within your environment, the table can also include Physical Sensors associated with the chassis object for performance monitoring and thresholds (click here for more information):

- Backplane Utilization

  Threshold based on the percentage of backplane usage compared to the total amount of available backplane resources.

Tip: See "Physical Sensor Form" on page 244 for more details about the node sensor attributes that appear in this view's column headings. Node Sensors are displayed in three views: "Physical Sensors View" on page 47, "Non-Normal Physical Sensors View" on page 394, and "Unmanaged Physical Sensors View" on page 585.

Physical Sensors Associated with this Chassis

Attribute	Description
Physical Sensors	Table view of the fault and performance metrics associated with the current card. You can use this table to determine the Status, Name, and Type for each Physical Sensor metric associated with the selected card. Double-click the row representing a Physical Sensor. The "Physical Sensor Monitored Attribute Form" on page 247 displays all details about the selected Node Sensor.

Physical Sensors Associated with this Chassis, continued

Attribute	Description
	Note: The NNMi administrator can set Physical Sensor thresholds. For more information, see "Chassis Form: Physical Sensors Tab" on page 204 and "Card Form: Physical Sensors Tab" on the previous page.

Card Form: Node Sensors Tab

The "Card Form" on page 211 provides details about the selected card.

For information about each tab:

The Card Form: Node Sensors tab displays a table of any Node Sensors associated with the card object for fault monitoring. Each Node Sensor identifies the health aspect that is being monitored.

(*NNM iSPI Performance for Metrics*) If the HPE Network Node Manager iSPI Performance for Metrics Software is installed and configured within your environment, the table can include Node Sensors associated with the card object for performance monitoring and thresholds (click here for more information):

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

Tip: See "Node Sensor Form" on page 232 for more details about the node sensor attributes that appear in this view's column headings. Node Sensors are displayed in three views: "Node Sensors View" on page 47, "Non-Normal Node Sensors View" on page 393, and "Unmanaged Node Sensors View" on page 585.

Node Sensors Associated with this Chassis

Attribute	Description
Node Sensors	Table view of fault and performance metrics associated with the current card. You can use this table to determine the Status, Name, and Type for each Node Sensor metric associated with the selected card. Double-click the row representing a Node Sensor. The "Node Sensor Form" on page 232 displays all details about the selected Node Sensor. **Note:** The NNMi administrator can set Node Sensor thresholds. For more information, see

Node Sensors Associated with this Chassis, continued

Attribute	Description
	"Node Form: Node Sensors Tab" on page 84, "Chassis Form: Node Sensors Tab" on page 205, and "Card Form: Node Sensors Tab" on the previous page.

Card Form: Incidents Tab

The "Card Form" on page 211 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 437 displays all details about the selected incident. **Tip:** See "Incident Form" on page 437 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 211 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: No Status Normal Disabled Unknown Warning

Overall Status Attributes, continued

Attribute	Description
	Minor Major Critical See "Watch Status Colors" on page 406 for more information about possible status values. Physical Component status is derived from SNMP polling results for Administrative State, Operational State, and the most serious outstanding conclusion. For information about how the current status was determined, see the following: • "Card Form: Conclusions Tab" on the next page • "Chassis Form: Conclusions Tab" on page 208 **Note:** The icons are displayed only in table views.
Status Last Modified	Date and time indicating when the Status was last set.

Physical Component Status History Table

Attribute	Description
Status History	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. Double-click the row representing a Status History. The "Physical Component Status History Form (Card)" below displays all details about the selected Status.

Physical Component Status History Form (Card)

Status is derived from SNMP polling results for Administrative State, Operational State, and the most serious outstanding conclusion.

See the object's conclusions for information about how the current status was determined:

- "Card Form: Conclusions Tab" on the next page

Status Attributes

Attribute	Description
Status	Overall status for the current chassis. See "Watch Status Colors" on page 406 for more information about possible status values. NNMi follows the ISO standard for status classification. Possible values are: No Status

Status Attributes, continued

Attribute	Description
	Normal Disabled Unknown Warning Minor Major Critical Physical Component status is derived from SNMP polling results for Administrative State, Operational State, and the most serious outstanding conclusion. **Note:** The icons are displayed only in table views. For more information see the following: • "Card Form: Status Tab" on page 224
Status Last Modified	Date and time indicating when the status was last set.

Card Form: Conclusions Tab

The "Card Form" on page 211 provides details about the selected card.

For information about each tab:

Outstanding Status Conclusion Values

Attribute	Description
Outstanding Status Conclusions	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 **Causal Engine**[1]. Each Conclusion listed is outstanding and contributes to the current overall Status. 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. Card Status is derived from the most serious outstanding Conclusion and SNMP polling

[1]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
	results for Administrative State and Operational State. Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion. The following table describes the possible Conclusions that might appear for a Card object. **Note:** A **Y** in the **Incident?** column indicates that the Conclusion results in an incident. **Critical Status Conclusions** **Disabled Status Conclusions** **Major Status Conclusions** **Minor Status Conclusions**

Critical Status Conclusions

Conclusion	Description	Status	Incident?
CardDown	The Operational State of the selected card is Down.	Critical	Y

Disabled Status Conclusions

Conclusion	Description	Status	Incident?
CardDisabled	SNMP agent reports that the Administrative State for the selected card is Down.	Disabled	Y

Major Status Conclusions

Conclusion	Description	Status	Incident?
CardWithBadBackplane	One or more backplanes have one or more monitored attributes that are outside the currently configured threshold range.	Major	N
CardWithBadFan	One or more fans are out of range or malfunctioning.	Major	N
CardWithBadPowerSupply	One or more power supplies are out of range or malfunctioning.	Major	N
CardWithBadTemperature	One or more temperature sensors are out of range or malfunctioning.	Major	N
CardWithBadVoltage	One or more voltage sensors are out of range or malfunctioning.	Major	N

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
CardUndeterminedState	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.	Minor	Y
DaughterCardsDown	The Operational State of at least one of the associated child cards is Down.	Minor	N

Unknown Status Conclusions

Conclusion	Description	Status	Incident?
CardUnmanageable	The SNMP agent of the managing Node is not responding.	Unknown	N

Normal Status Conclusions

Conclusion	Description	Status	Incident?
CardUp	The Operational State for the current card is Up.	Normal	N
DaughterCardsUp	The Operational State of all associated child cards are Up.	Normal	N

Physical Component Status Conclusions Form (Card)

The current Conclusion contributes towards the current overall Status of the selected Physical Component.

Basics Attributes

Attribute	Description
Status	Status is derived from the most serious outstanding Conclusion and SNMP polling results for Administrative State and Operational State.
Time Stamp	The time of the last change in Status.

Basics Attributes, continued

Attribute	Description
Conclusion	For more information about each conclusion, see the following: • "Card Form: Conclusions Tab" on page 226

Card Form: RegistrationTab

The "Card Form" on page 211 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. **Note:** This value does not change when a node is rediscovered. This is because the Node object is modified, but not created.
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. Note the following: • 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. • 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.

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 <*Card-number / Port-number*>.
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** **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	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 Click the Lookup icon and select Show Analysis or Open to display more information about the interface.

Basic Attributes, continued

Attribute	Description
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 65

"Interface Form" on page 113

"Card Form" on page 211

Port Form: VLANs Tab

The "Port Form" on page 229 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 191 displays all details about the selected VLAN.

Related Topics:

"Node Form" on page 65

"VLAN Form" on page 191

Port Form: RegistrationTab

The "Port Form" on page 229 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. **Note:** This value does not change when a node is rediscovered. This is because the Node object is modified, but not created.
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. Note the following: • 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. • 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.

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 Sensor Form

This form describes the fault and performance metrics used to monitor Node Sensors. NNMi obtains fault metrics from the node's SNMP agent (MIB files).

For information about each tab:

Tip: Node Sensors are displayed in three views: "Node Sensors View" on page 47, "Non-Normal Node Sensors View" on page 393, and "Unmanaged Node Sensors View" on page 585.

Basic Attributes

Attribute	Description
Status	Overall status for the current Node Sensor. NNMi follows the ISO standard for status classification. See Status Color for Objects for more information. Possible values are: No Status Normal Disabled

Basic Attributes, continued

Attribute	Description
	Unknown Warning Minor Major Critical For information about how the current status was determined, see the Conclusions tab. Status reflects the most serious outstanding conclusion. See "Watch Status Colors" on page 406 for more information about possible status values. **Note:** The icons are displayed only in table views.
Name	Name of the Node Sensor that has the health attribute being measured, For example, NNMi measures fault metrics. (*NNM iSPI Performance for Metrics*) If licensed and installed, HPE Network Node Manager iSPI Performance for Metrics Software also measures performance metrics for CPU, disk, memory, and buffer utilization as well as for buffer failures and misses. When possible, NNMi obtains the Name value for the Node Sensor from the associated SNMP agent. The number of MIBs available and subsequently the number of health attributes that are measured for each Node Sensor vary. For example, if the Node Sensor is of type Buffer, up to five MIBs that contain information about Buffers (Small, Medium, Large, Big, and Huge). NNMi collects information from each MIB that is available and lists a Node Sensor Name value for each. For example, If all five MIBs are available, you see the following Node Sensors listed in the Node Sensor table: Small Buffers, Medium Buffers, Large Buffers, Big Buffers, and Huge Buffers. **Note:** If the associated MIB file does not provide a name value, NNMi uses the value provided by the Type attribute.

Type	Identifies the health aspect that is being monitored.
	(*NNM iSPI Performance for Metrics*) The following examples require an HPE Network Node Manager iSPI Performance for Metrics Software license:
	• Buffer
	  • Buffer Failure Rate
	  • Buffer Miss Rate
	  • Buffer Utilization
	• CPU utilization

Basic Attributes, continued

Attribute	Description
	• CPU 1Min Utilization • CPU 5Min Utilization • CPU 5Sec Utilization • Disk Space Utilization • Memory Utilization
Management Mode	The *calculated* Management Mode for the node sensor according to the Management Mode Hierarchy. This value reflects the current management mode of this node sensor's parent object (the Hosted On Node). See "How NNMi Assigns the Management Mode to an Object" on page 591. (*NNMi Advanced - Global Network Management feature*) 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. **Note:** If the NNMi Security configuration permits, you can change this setting using **Actions** → **Management Mode**. **Tip:** You can also right-click any object in a table or map view to access the items available within the **Actions** menu.
Direct Management Mode	Indicates whether or not NNMi is currently monitoring the node sensor. Possible values are: **Inherited** – Used to indicate that the Node Sensor should inherit the Management Mode from this node sensor's parent object (the Hosted On Node). **Not Managed** – Used to indicate that NNMi does not discover or monitor the Node Sensor. **Out of Service** – Used to indicate a Node Sensor is unavailable because it is out of service or participating in a Scheduled Node Outage. NNMi does not discover or monitor this Node Sensor. NNMi administrators and Level 2 Operators can use the drop-down selection list to change the current setting. **Note:** If you change the Direct Management Mode using **Actions** → **Management Mode**, NNMi updates the calculated Management Mode on the form. If you manually set the Direct Management Mode and then Save your changes, the Management Mode value is not updated until you refresh the form.
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. See "Node Form" on page 65 for more

Basic Attributes, continued

Attribute	Description
	information. **Note:** The NNMi administrator can set Physical Sensor thresholds. For more information, see "Node Form: Node Sensors Tab" on page 84, "Chassis Form: Node Sensors Tab" on page 205 and "Card Form: Node Sensors Tab" on page 223.

Node Sensor Form: Monitored Attributes Tab

The "Node Sensor Form" on page 232 provides details about the monitored attributes (for example, Memory Utilization) related to the current Node Sensor. The State of monitored attributes can be influenced by thresholds configured by your NNMi administrator.

For information about each tab:

Attributes Table

Description
Table view of the Name, State, and Last Modified time for each monitored attribute associated with the selected Node Sensor. Use this view to determine the State of each monitored attribute. Double-click the row representing a Monitored Attribute. The "Node Sensor Monitored Attribute Form" below displays all details about the selected Monitored Attribute.

Node Sensor Monitored Attribute Form

The Node Sensor Monitored Attribute form displays information about the attribute selected on the "Node Sensor Form: Monitored Attributes Tab" above.

NNMi obtains fault metric information from the associated MIB.

(*NNM iSPI Performance for Metrics*) If the HPE Network Node Manager iSPI Performance for Metrics Software is installed and configured within your environment, the Node Component: Monitored Attributes tab also displays information about node health related to the following performance metrics. The NNMi administrator sets the threshold for node sensors related to performance metrics:

- 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
Label	Name used to identify the attribute being monitored. See "Node Sensor Form" on page 232 for more information. 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: • CPU Revised 1 Minute • CPU Revised 5 Minute • CPU Revised 5 Second
Unique Key	Used as a unique identifier for the Monitored Attribute. Any Monitored Attribute provided by NNMi begins with the prefix `com.hp.nms`.
State	Normalized value used to indicate the State of the attribute of the selected Monitored Attribute. Possible values are listed below. **Note:** The NNMi State Poller interprets and normalizes the State value returned for the Monitored Attribute to handle the differences between vendor-specific nodes. **Normal** - Indicates there are no known problems related to the associated object. **Warning** - Indicates there might be a problem related to the associated object. **Minor** - Indicates NNMi has detected problems related to the associated object that require further investigation. **Major** - Indicates NNMi detected problems that could precede a critical situation. **Critical** - Indicates NNMi detected problems that require immediate attention. The following values indicate NNMi could not gather the required data: **Agent Error** – Indicates an error was returned in response to the query. **No Polling Policy** - No polling policy exists for this monitored attribute. **Not Polled** - 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. **Not Provided** — The device does not support providing information for this monitored attribute. **Unavailable** - The agent responded with a value outside the range of possible values or returned a null value.

Basics Attributes, continued

Attribute	Description
	Unset – Currently not used by NNMi. (*NNM iSPI Performance for Metrics*) Additional States for performance metrics include the following (**Warning** and **Critical** states are not used for performance metrics): **Abnormal Range** – Indicates State Poller has collected values outside the normal range when compared to the baseline data collected for the current object. **Normal** - Indicates there are no known problems related to the associated object. **Normal Range** - Indicates State Poller collected values within the normal range when compared to the baseline data collected for the current object. **High** - The High threshold was crossed. **Low** - The Low threshold was crossed. **None** - The threshold value returned is zero.
Last Modified	The most recent date and time when the State of this Monitored Attribute changed.

Node Sensor Form: Physical Components Tab

The "Node Sensor Form" on page 232 provides details about the monitored attribute (for example, Memory Utilization) related to the current Node Sensor.

For information about each tab:

Physical Components Table

Description
Table of all of the Physical Components (Chassis and Cards) that are associated with the selected Node Sensor. Use this table to access information about each Chassis or Card that is associated with the selected Node Sensor. The information displayed includes, but is not limited to, the physical component State, Status, model, type, and serial number, as well as the firmware, software, and hardware version. Double-click the row representing a the Physical Component of interest. The "Chassis Form" on page 193 displays all details about the selected Chassis. The "Card Form" on page 211 displays all details about the selected Card.

Node Sensor Form: Incidents Tab

The "Node Sensor Form" on page 232 provides details about the selected node sensor.

For information about each tab:

Incidents Associated with this Node Sensor

Attribute	Description
Incidents	Table of the Incidents associated with the selected node sensor. 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 node sensor Double-click the row representing an incident. The "Incident Form" on page 437 displays all details about the selected incident. **Tip:** See "Incident Form" on page 437 for more details about the incident attributes that appear in the incident table's column headings.

Node Sensor Form: Status Tab

The "Node Sensor Form" on page 232 provides details about the selected Node Sensor.

For information about each tab:

Overall Status

Attribute	Description
Status	Overall status for the current Node Sensor. NNMi follows the ISO standard for status classification. Possible values are: No Status Normal Disabled Unknown Warning Minor Major Critical **Note:** Your NNMi administrator might have disabled polling of Node Sensors using the Monitoring Configuration workspace. The status of the Node Sensor contributes to the parent Node's overall status. For information about how the current status was determined, see the "Node Sensor Form: Conclusions Tab" on page 240. Status reflects the most serious outstanding conclusion. See "Watch Status Colors" on page 406 for more information about possible status values.

Overall Status, continued

Attribute	Description
	Note: The icons are displayed only in table views.
Status Last Modified	Date and time indicating when the status was last set.

Status History Table

Attribute	Description
Status History	List of the last 30 changes in the status for the Node Sensor. This view is useful for obtaining a summary of the Node Sensor status so that you can better determine any patterns in behavior and activity. Double-click the row representing a Status History. The "Node Sensor Status History Form" below displays all details about the selected Status.

Node Sensor Status History Form

The Node Sensor Status History form displays information about the selected Status History entry on the "Node Sensor Form: Status Tab " on the previous page.

Overall Status

Attribute	Description
Status	Status for the selected Status History entry. NNMi follows the ISO standard for status classification. Possible values are: No Status Normal Disabled Unknown Warning Minor Major Critical **Note:** Your NNMi administrator might have disabled polling of Node Sensors using the

Overall Status, continued

Attribute	Description
	Monitoring Configuration workspace. The status of the Node Sensor contributes to the parent Node's overall status. For information about how the current status was determined, see the "Node Sensor Form: Conclusions Tab" below. Status reflects the most serious outstanding conclusion. See "Watch Status Colors" on page 406 for more information about possible status values. **Note:** The Status icons are displayed only in table views.
Time Stamp	Date and time indicating when the Status History entry was established.

Node Sensor Form: Conclusions Tab

The "Node Sensor Form" on page 232 provides details about the selected health metric for the current Node Sensor.

For information about each tab:

Outstanding Status Conclusion Values

Attribute	Description
Outstanding Status Conclusions	The dynamically generated list of summary statuses of the monitored attribute that contributed to the current overall status of the selected Node Sensor. Status is set by the Causal Engine. Each Conclusion listed is outstanding and contributes to the current overall Status. This view is useful for obtaining a quick summary of the problem description for the current monitored attribute that led up to the Node Sensor's most current Status. The status value is correlated based on the most critical conclusions. Double-click the row representing a Status Conclusion. The "Node Sensor Status Conclusion Form" on page 243 displays all details about the selected Status Conclusion. The following table describes the possible Conclusions that might appear for a Node Sensor object. **Note:** A **Y** in the **Incident?** column indicates that the Conclusion results in an incident. **Critical Status Conclusions**

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
BufferOutOfRangeOrMalfunctioning	The buffer pool monitored attributes are outside of the threshold range configured for the device. This incident indicates the buffer pool is exhausted or cannot meet the demand.	Critical	Y
CpuOutOfRangeOrMalfunctioning	Any of the following utilization averages is above the threshold range configured for the device: • CPU 5 second utilization • CPU 1 minute utilization • CPU 5 minute utilization	Critical	Y
DiskOutOfRangeOrMalfunctioning	The disk monitored attributes are outside of the threshold range configured for the device.	Critical	Y
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

Warning Status Conclusions

Conclusion	Description	Status	Incident?
BufferAbnormal	The buffer utilization is abnormal based on	Warning	Y

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	the computed baseline.		
CpuAbnormal	The CPU utilization is abnormal based on the computed baseline for one of the following: • CPU 5 second utilization • CPU 1 minute utilization • CPU 5 minute utilization	Warning	Y
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

Normal Status Conclusions

Conclusion	Description	Status	Incident?
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 threshold range configured for the device: • CPU 5 second utilization • CPU 1 minute utilization • CPU 5 minute utilization	Normal	N
CpuNormal	The CPU utilization is normal based on the computed baseline for the following: • CPU 5 second utilization • CPU 1 minute utilization • CPU 5 minute utilization	Normal	N

Outstanding Status Conclusion Values, continued

Attribute	Description
	<table><tr><th>Conclusion</th><th>Description</th><th>Status</th><th>Incident?</th></tr><tr><td>DiskInRangeAndFunctioning</td><td>The disk monitored attributes are within the threshold range configured for the device.</td><td>Normal</td><td>N</td></tr><tr><td>DiskNormal</td><td>The disk space utilization is normal based on the computed baseline.</td><td>Normal</td><td>N</td></tr><tr><td>MemoryInRangeAndFunctioning</td><td>The specified memory pool is operating within the threshold range configured for the device.</td><td>Normal</td><td>N</td></tr><tr><td>MemoryNormal</td><td>The memory utilization is normal based on the computed baseline.</td><td>Normal</td><td>N</td></tr></table>

Node Sensor Status Conclusion Form

The current Conclusion contributes towards the overall Status of the selected Node Sensor (see "Node Sensor Form: Status Tab " on page 238).

Outstanding Status Conclusion Values

Attribute	Description
Time Stamp	The time of the last change in Status.
Conclusion	For more information see the "Node Sensor Form: Conclusions Tab" on page 240.

Node Sensor Form: Registration Tab

The "Node Sensor Form" on page 232 provides details about the selected Node Sensor.

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. **Note:** This value does not change when a node is rediscovered. This is because the Node object is modified, but not created.

Registration Attributes, continued

Attribute	Description
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. Note the following: • 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. • 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.

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.

Physical Sensor Form

This form describes the fault and performance metrics used to monitor Physical Sensors. NNMi obtains fault metrics from the node's SNMP agent (MIB files).

For information about each tab:

Tip: The NNMi administrator can set Physical Sensor thresholds. Physical Sensors are displayed in three views: "Physical Sensors View" on page 47, "Non-Normal Physical Sensors View" on page 394, and "Unmanaged Physical Sensors View" on page 585.

Basic Attributes

Attribute	Description
Status	Overall status for the current Physical Sensor. NNMi follows the ISO standard for status classification. See Status Color for Objects for more information. Possible values are: No Status Normal Disabled Unknown Warning Minor

Basic Attributes, continued

Attribute	Description
	Major Critical For information about how the current status was determined, see the Conclusions tab. Status reflects the most serious outstanding conclusion. See "Watch Status Colors" on page 406 for more information about possible status values. **Note:** The icons are displayed only in table views.
Name	Name of the Physical Sensor that has the health attribute being measured, For example, NNMi measures fault metrics for Fan, Power Supply, Temperature, and Voltage. (*NNM iSPI Performance for Metrics*) If licensed and installed, HPE Network Node Manager iSPI Performance for Metrics Software also measures performance metrics for Backplane. When possible, NNMi obtains the Name value for the Physical Sensor from the associated SNMP agent. The number of MIBs available and subsequently the number of health attributes that are measured for each Physical Sensor vary. **Note:** If the associated MIB file does not provide a name value, NNMi uses the value provided by the Type attribute.
Type	Identifies the health aspect that is being monitored. Possible values include: • Fan • Power Supply • Temperature • Voltage (*NNM iSPI Performance for Metrics*) Health monitoring of the following requires an HPE Network Node Manager iSPI Performance for Metrics Software license: • Backplane
Management Mode	The *calculated* Management Mode for the physical sensor according to the Management Mode Hierarchy. This value reflects the current management mode of this physical sensor's parent object (either the Hosted On chassis or card, or the Managed By node). See "How NNMi Assigns the Management Mode to an Object" on page 591. (*NNMi Advanced - Global Network Management feature*) 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. **Note:** If the NNMi Security configuration permits, you can change this setting using **Actions → Management Mode**.

Basic Attributes, continued

Attribute	Description
	Tip: You can also right-click any object in a table or map view to access the items available within the **Actions** menu.
Direct Management Mode	Indicates whether or not NNMi is currently monitoring the physical sensor. Possible values are: **Inherited** – Used to indicate that the Physical Sensor should inherit the Management Mode from the physical sensor's parent object (either the Hosted On chassis or card, or the Managed By node). **Not Managed** – Used to indicate that NNMi does not discover or monitor the Physical Sensor. **Out of Service** – Used to indicate a Physical Sensor is unavailable because it is out of service or participating in a Scheduled Node Outage. NNMi does not discover or monitor this Physical Sensor. NNMi administrators and Level 2 Operators can use the drop-down selection list to change the current setting. **Note:** If you change the Direct Management Mode using **Actions** → **Management Mode**, NNMi updates the calculated Management Mode on the form. If you manually set the Direct Management Mode and then Save your changes, the Management Mode value is not updated until you refresh the form.
Managed By	The node using this chassis or the node assigned to the Agent that is managing this chassis. This is the current value in NNMi's database for the Name attribute of the host 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). Click the Lookup icon and select Show Analysis or Open to display more information about the node.
Hosted On	Chassis or card on which the health metric is being measured. This is the current value in NNMi's database for the Name attribute of the chassis or card. See "Chassis Form" on page 193 or Card Form for more information. **Note:** The NNMi administrator can set Physical Sensor thresholds. For more information, see "Chassis Form: Physical Sensors Tab" on page 204 and "Card Form: Physical Sensors Tab" on page 222.

Physical Sensor Form: Monitored Attributes Tab

The "Physical Sensor Form" on page 244 provides details about the monitored attributes related to the current Physical Sensor. The State of monitored attributes can be influenced by thresholds configured by your NNMi

administrator.

For information about each tab:

Attributes Table

Description
Table view of the Name, State, and Last Modified time for each monitored attribute associated with the selected Physical Sensor. Use this view to determine the State of each monitored attribute. Double-click the row representing a Monitored Attribute. The "Physical Sensor Monitored Attribute Form" below displays all details about the selected Monitored Attribute.

Physical Sensor Monitored Attribute Form

The Physical Sensor Monitored Attribute form displays information about the attribute selected on the "Physical Sensor Form: Monitored Attributes Tab" on the previous page.

Physical Sensors for fault monitoring include the following:

- Fan
- Power Supply
- Temperature
- Voltage

(*NNM iSPI Performance for Metrics*) If the HPE Network Node Manager iSPI Performance for Metrics Software is installed and configured within your environment, the NNMi administrator can also configure Performance monitoring and thresholds for the following:

- Backplane Utilization

  Threshold based on the percentage of backplane usage compared to the total amount of available backplane resources.

NNMi obtains fault metric information from the associated MIB.

Basics Attributes

Attribute	Description
Label	Name used to identify the attribute being monitored. The Name of each health attribute identifies the attribute being measured as well as the type of MIB used to gather this information.
Unique Key	Used as a unique identifier for the Monitored Attribute. Any Monitored Attribute provided by NNMi begins with the prefix `com.hp.nms`.
State	Normalized value used to indicate the State of the attribute of the selected node. Possible values are listed below. **Note:** The NNMi State Poller interprets and normalizes the State value returned for the monitored attribute to handle the differences between vendor-specific nodes.

Basics Attributes, continued

Attribute	Description
	Normal - Indicates there are no known problems related to the associated object. **Warning** - Indicates there might be a problem related to the associated object. **Minor** - Indicates NNMi has detected problems related to the associated object that require further investigation. **Major** - Indicates NNMi detected problems that could precede a critical situation. **Critical** - Indicates NNMi detected problems that require immediate attention. The following values indicate NNMi could not gather the required data: **Agent Error** – Indicates an error was returned in response to the query. **No Polling Policy** - No polling policy exists for this monitored attribute. **Not Polled** - 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. **Not Provided** — The device does not support providing information for this monitored attribute. **Unavailable** - The agent responded with a value outside the range of possible values or returned a null value. **Unset** – Currently not used by NNMi. **Note:** State is determined by the State Poller Service. Only the Physical Sensor States for Fan and Power Supply contribute towards the status calculation for the host node. See the Status tab for more information. (*NNM iSPI Performance for Metrics*) Additional States for performance metrics include the following (**Warning** and **Critical** states are not used for performance metrics): **Abnormal Range** – Indicates State Poller has collected values outside the normal range when compared to the baseline data collected for the current object. **Normal** - Indicates there are no known problems related to the associated object. **Normal Range** - Indicates State Poller collected values within the normal range when compared to the baseline data collected for the current object. **High** - The High threshold was crossed. **Low** - The Low threshold was crossed. **None** - The threshold value returned is zero.

Basics Attributes, continued

Attribute	Description
Last Modified	The most recent date and time when the State of this Monitored Attribute changed.

Physical Sensor Form: Incidents Tab

The "Physical Sensor Form" on page 244 provides details about the selected physical sensor.

For information about each tab:

Incidents Associated with this Physical Sensor

Attribute	Description
Incidents	Table of the Incidents associated with the selected physical sensor. 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 physical sensor Double-click the row representing an incident. The "Incident Form" on page 437 displays all details about the selected incident. **Tip:** See "Incident Form" on page 437 for more details about the incident attributes that appear in the incident table's column headings.

Physical Sensor Form: Status Tab

The "Physical Sensor Form" on page 244 provides details about the selected Physical Sensor.

For information about each tab:

Overall Status

Attribute	Description
Status	Overall status for the current Physical Sensor. NNMi follows the ISO standard for status classification. Possible values are: No Status Normal Disabled Unknown Warning Minor

Overall Status, continued

Attribute	Description
	Major Critical **Note:** Your NNMi administrator might have disabled polling of Physical Sensors using the Monitoring Configuration workspace. The status of the Physical Sensor contributes to the parent Chassis's overall status. For information about how the current status was determined, see the "Physical Sensor Form: Conclusions Tab" on the next page. Status reflects the most serious outstanding conclusion. See "Watch Status Colors" on page 406 for more information about possible status values. **Note:** The icons are displayed only in table views.
Status Last Modified	Date and time indicating when the status was last set.

Status History Table

Attribute	Description
Status History	List of the last 30 changes in the status for the Physical Sensor. This view is useful for obtaining a summary of the Physical Sensor status so that you can better determine any patterns in behavior and activity. Double-click the row representing a Status History. The "Physical Sensor Status History Form" below displays all details about the selected Status.

Physical Sensor Status History Form

The Physical Sensor Status History form displays information about the selected Status History entry on the "Physical Sensor Form: Status Tab " on the previous page.

Overall Status

Attribute	Description
Status	Status for the selected Status History entry. NNMi follows the ISO standard for status classification. Possible values are: No Status Normal

Overall Status, continued

Attribute	Description
	Disabled Unknown Warning Minor Major Critical **Note:** Your NNMi administrator might have disabled polling of Physical Sensors using the Monitoring Configuration workspace. The status of the Physical Sensor contributes to the parent Chassis's overall status. For information about how the current status was determined, see the "Physical Sensor Form: Conclusions Tab" below. Status reflects the most serious outstanding conclusion. See "Watch Status Colors" on page 406 for more information about possible status values. **Note:** The Status icons are displayed only in table views.
Time Stamp	Date and time indicating when the Status History entry was established.

Physical Sensor Form: Conclusions Tab

The "Physical Sensor Form" on page 244 provides details about the selected health metric for the current Physical Sensor.

For information about each tab:

Outstanding Status Conclusion Values

Attribute	Description
Outstanding Status Conclusions	The dynamically generated list of summary statuses of the monitored attribute that contributed to the current overall status of the selected Physical Sensor. Status is set by the Causal Engine. Each Conclusion listed is outstanding and contributes to the current overall Status. This view is useful for obtaining a quick summary of the problem description for the current monitored attribute that led up to the Physical Sensor's most current Status. The status value is correlated based on the most critical conclusions. Double-click the row representing a Status Conclusion. The "Physical Sensor Status

Outstanding Status Conclusion Values, continued

Attribute	Description
	Conclusions Form" on page 254 displays all details about the selected Status Conclusion. The following table describes the possible Conclusions that might appear for a Physical Sensor object. **Note:** A **Y** in the **Incident?** column indicates that the Conclusion results in an incident.

Critical Status Conclusions

Conclusion	Description	Status	Incident?
BackplaneOutOfRangeOrMalfunctioning	The backplane monitored attributes are outside of the threshold range configured for the device.	Critical	Y
FanOutOfRangeOrMalfunctioning	The fan monitored attributes are outside of the threshold range configured for the device.	Critical	Y
PowerSupplyOutOfRangeOrMalfunctioning	A power supply's monitored attributes are outside of the threshold range configured for the device.	Critical	Y
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	Critical	Y

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	configured for the device.		

Warning Status Conclusions

Conclusion	Description	Status	Incident?
BackplaneAbnormal	The backplane utilization is abnormal based on the computed baseline.	Warning	Y

Normal Status Conclusions

Conclusion	Description	Status	Incident?
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
FanInRangeAndFunctioning	The specified fan monitored attributes are within the threshold range configured for the device.	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

Physical Sensor Status Conclusions Form

The current Conclusion contributes towards the overall Status of the selected Physical Sensor (see "Physical Sensor Form: Status Tab " on page 249).

Outstanding Status Conclusion Values

Attribute	Description
Time Stamp	The time of the last change in Status.
Conclusion	For more information see the "Physical Sensor Form: Conclusions Tab" on page 251.

Physical Sensor Form: Registration Tab

The "Physical Sensor Form" on page 244 provides details about the selected Physical Sensor.

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. **Note:** This value does not change when a node is rediscovered. This is because the Node object is modified, but not created.
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. Note the following: • 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. • 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.

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: *Node_Name*[*Interface_Name*].
Status	Overall status for the current connection. NNMi follows the ISO standard for status classification. See the "Layer 2 Connection Form: Status Tab" on page 258 for more information. Possible values are: No Status Normal Disabled Unknown Warning Minor Major Critical

Basic Attributes, continued

Attribute	Description
	For information about how the current status was determined, see the "Layer 2 Connection Form: Conclusions Tab" on page 260. Status reflects the most serious outstanding conclusion. See "Watch Status Colors" on page 406 for more information about possible status values. **Note:** The icons are displayed only in table views.
Topology Source	Indicates the data source used to create this connection. **Note:** (*NNMi Advanced*) Layer 2 Connections using **Link Aggregation**[1] or **Split Link Aggregation**[2] protocols can connect *sets* of Interfaces. See "Layer 2 Connection Form: Link Aggregation Tab (NNMi Advanced)" on page 265. These Aggregator Layer 2 Connections display as thick lines on NNMi maps. If you see the icon (in previous NNMi releases 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 (LLC) sub-layer controls frame synchronization, flow control, and error checking. The following are some examples of possible Topology Source values: **CDP** - Cisco Discovery Protocol. On the NNMi map, the following icon is in the middle of the Layer 2 Connection line: **EDP** - Extreme Discovery Protocol **EnDP** - Enterasys Discovery Protocol (also known as CDP - Cabletron Discovery Protocol) **FDB** - Forwarding Database (also known as AFT - Address Forwarding Table on a switch). On the NNMi map, the following icon is in the middle of the Layer 2 Connection line: (in prior NNMi releases, the icon) **FDBH** - NNMi's Forwarding Database High Priority indicates a special case was encountered and NNMi gave priority of FDB over Discovery Protocol information. **FDP** - Foundry Discovery Protocol **IEEELAG** - Institute of Electrical and Electronics Engineers Link Aggregation

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

Basic Attributes, continued

Attribute	Description
	ISL - Inter Switch Link Protocol **LLDP** - Link Layer Discovery Protocol **NDP** - IPv6 Neighbor Discovery Protocol **SONMP** - SynOptics Network Management Protocol **VMWARE** - VMware VSphere® web-service **ROUTES** - Indicates that an unnumbered Interface is involved in this connection. The NNMi administrator has enabled the Unnumbered Interface Connectivity feature. For more information: **SUBNETCONNECTION** - 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: (in prior NNMi releases, the icon) **USER** - This connection was configured by your NNMi administrator (using the Connection Editor). See "Help for Administrators" for more information.
Notes	(*NNMi Advanced - Global Network Management feature*) 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 Layer 2 Connection. Information might include when a cable was last replaced. 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 255 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	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. Double-click the row representing an interface. The "Interface Form" on page 113 displays all details about the selected interface.

Layer 2 Connection Form: Incidents Tab

The "Layer 2 Connection Form" on page 255 provides details about a managed connection.

For information about each tab:

Incidents Table

Attribute	Description
Associated Incidents	Table view of the incidents associated with the selected Layer 2 Connection. NNMi displays only those incidents that have a Family attribute value of `Connection`. **Tip:** To check all Incidents related to the Interface on each end of the connection, navigate to the "Layer 2 Connection Form: Interfaces Tab" on the previous page and open an Interface form. To check all incidents related to the Node, use the **Hosted On Node** attribute on the Interface form to open the Node form. Examples of the incidents that might appear as Associated Incidents for Layer 2 Connections include the following: • "Connection Down" on page 507 • Modified Connection Down 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. Double-click the row representing an incident. The "Incident Form" on page 437 displays all details about the selected incident. Navigate to the "Incident Form: Correlated Children Tab" on page 446 and "Incident Form: Correlated Parents Tab" on page 446 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 255 provides details about a managed connection.

For information about each tab:

Status Attributes

Attribute	Description
Status	Overall status for the current connection. NNMi follows the ISO standard for status classification. Possible values are: **Note:** The icons are displayed only in table views. No Status Normal Disabled Unknown Warning Minor Major Critical 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 406 for more information about possible status values. (*NNMi Advanced*) **Link Aggregation**[1] or **Split Link Aggregation**[2]: 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 "Layer 2 Connection Form: Link Aggregation Tab (NNMi Advanced)" on page 265 and Status Color for Aggregator Objects.
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

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

Status History Table, continued

Attribute	Description
	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 255 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. 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. The Status value is correlated based on the most critical Conclusion. Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion. The following table describes the possible Conclusions that might appear for a Connection object. **Note:** A **Y** in the **Incident?** column indicates that the Conclusion results in an incident. **Critical Status Conclusions**

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
AggregatorLinkDown	(*NNMi Advanced*) **Link Aggregation**[1] or **Split Link Aggregation**[2]: The Operational State of *all* participating Aggregation Member Layer 2 Connections is Down. For more information, see "Layer 2 Connection Form: Link Aggregation Tab (NNMi Advanced)" on page 265.	Critical	Y
AllConnectionThresholdValuesHigh	Each interface in the connection contains one of the following Conclusions:	Critical	N
	• InterfaceInputUtilizationHigh • InterfaceOutputUtilizationHigh • InterfaceInputDiscardRateHigh • InterfaceOutputDiscardRateHigh • InterfaceInputErrorRateHigh • InterfaceOutputErrorRateHigh • InterfaceOutputQueueDropsRateHigh • InterfaceInputQueueDropsRateHigh • InterfaceFCSWLANErrorRateHigh • InterfaceFCSLANErrorRateHigh		
ConnectionDown	Both (or all) ends of a connection have an Operational State of Down.	Critical	Y

Minor Status Conclusions

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
AggregatorLinkDegraded	(*NNMi Advanced*) **Link Aggregation**[1] or **Split Link Aggregation**[2]: Some (but not all) of the participating Aggregation Member Layer 2 Connections have an Operational State of Down. For more information, see "Layer 2 Connection Form: Link Aggregation Tab (NNMi Advanced)" on page 265.	Minor	Y
ConnectionWithAtLeastOneDownEP	At least one interface, but not all interfaces, in the connection have an	Minor	N

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	Operational State of Down.		
SomeConnectionThresholdValuesHigh	One interface in the connection contains one of the following conclusions:	Minor	N
	• InterfaceInputUtilizationHigh • InterfaceOutputUtilizationHigh • InterfaceInputDiscardRateHigh • InterfaceOutputDiscardRateHigh • InterfaceInputErrorRateHigh • InterfaceOutputErrorRateHigh • InterfaceOutputQueueDropsRateHigh • InterfaceInputQueueDropsRateHigh • InterfaceFCSWLANErrorRateHigh • InterfaceFCSLANErrorRateHigh		
SomeOrAllConnectionThresholdValuesLow	One Interface in the connection contains one of the following conclusions:	Minor	N
	• InterfaceInputUtilizationLow • InterfaceOutputUtilizationLow		
SomeOrAllConnectionThresholdValuesNone	One interface in the connection contains one of the	Minor	N

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	following conclusions:		
	• InterfaceInputUtilizationNone • InterfaceOutputUtilizationNone • InterfaceInputDiscardRateNone • InterfaceOutputDiscardRateNone • InterfaceInputErrorRateNone • InterfaceOutputErrorRateNone		

Warning Status Conclusions

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 SNMP queries.	Warning	N

Unknown Status Conclusions

Conclusion	Description	Status	Incident?
ConnectionUnknown	All SNMP Agents associated with all interfaces in the connection are not responding to SNMP queries.	Unknown	N

Disabled Status Conclusions

Conclusion	Description	Status	Incident?
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

Outstanding Status Conclusion Values, continued

Attribute	Description
	Normal Status Conclusions

Conclusion	Description	Status	Incident?
AggregatorLinkUp	(*NNMi Advanced*) **Link Aggregation**[1] or **Split Link Aggregation**[2]: All 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.	Normal	N
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

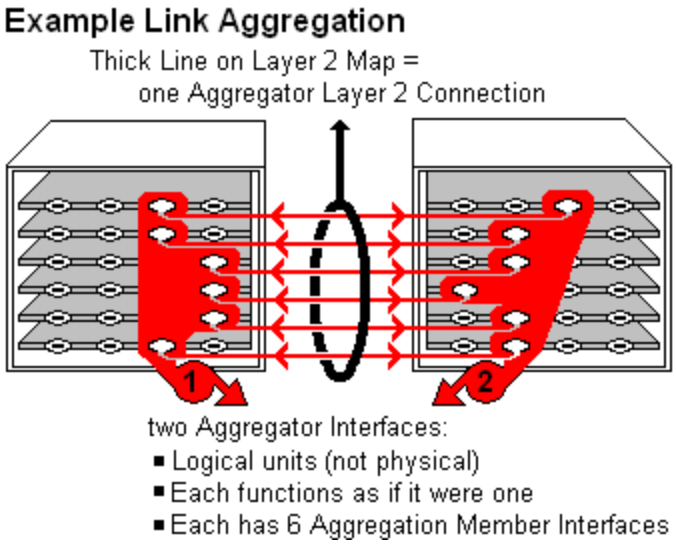
Layer 2 Connection Form: Link Aggregation Tab (*NNMi Advanced*)

The "Layer 2 Connection Form" on page 255 provides details about the selected Layer 2 Connection.

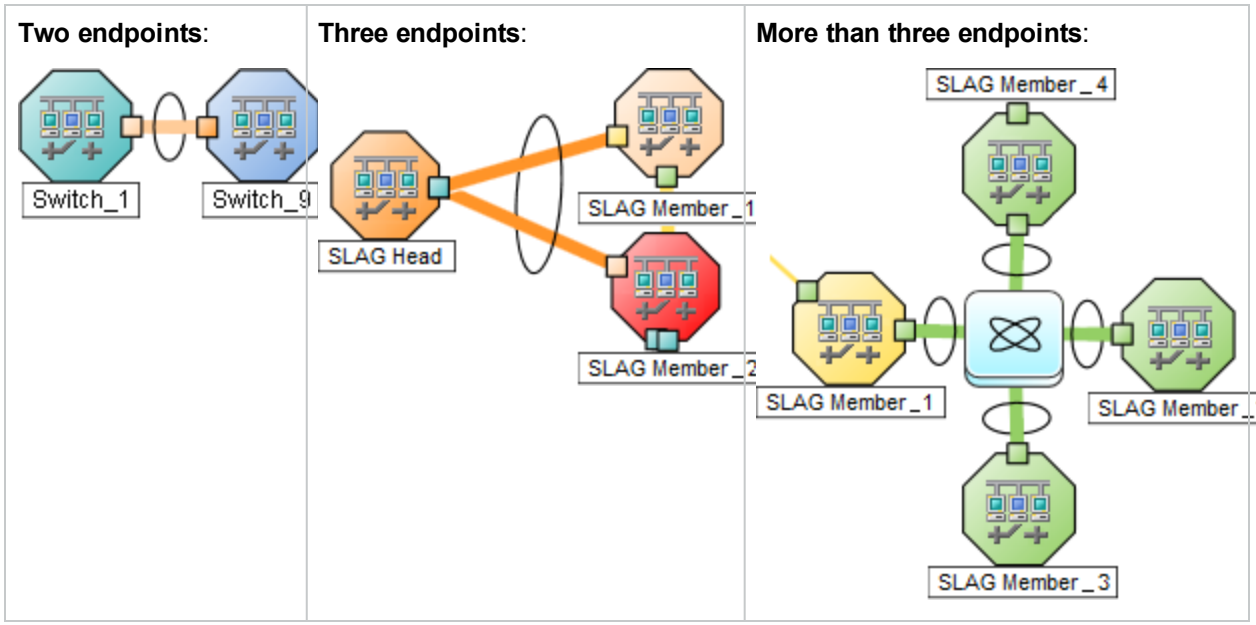
For information about each tab:

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

The Layer 2 Connection Form: Link Aggregation Tab appears if the selected connection uses a Link Aggregation protocol.



On a Layer 2 map, a thick line with a superimposed ellipse represents a **Link Aggregation**[1] or **Split Link Aggregation**[2] (group of multiple Layer 2 Connections that are functioning as one). The icon representing an Interface at either end of the thick line is an Aggregator Interface (a *logical* interface comprised of many physical interfaces that are functioning as one).



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

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

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

Attribute	Description
Link Aggregation Protocol	The **Link Aggregation**[1] or **Split Link Aggregation**[2] Protocol currently in use. These protocols allow network administrators to configure a *set of interfaces* on a switch as one *Aggregator Interface*, 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: **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 **Note:** 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 (/).
Aggregator	Name of the Aggregator that *contains* the selected participating Aggregation Member: • Aggregator Interface - represents multiple member interfaces • Aggregator Layer 2 Connection - thick line on the Layer 2 map represents multiple member Layer 2 Connections See Layer 2 Neighbor View Map Objects for more information. Click the Lookup icon, and choose Open to open the form for the Aggregator.

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

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

Attribute	Description
Link Aggregation Protocol	The **Link Aggregation**[1] or **Split Link Aggregation**[2] Protocol currently in use. These protocols allow network administrators to configure a *set of interfaces* on a switch as one *Aggregator Interface*, 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:
Available Bandwidth	Sum of the interface Input Speed attribute values of the Member Interfaces that have a MIB-II ifOperStatus that is not `Down`. 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.

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

Note: 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 (/).

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

Attribute	Description
Available Bandwidth Percentage	Percentage value computed using Available Bandwidth divided by the Maximum Bandwidth.
Members	Table view of the Aggregation Members. For more information, double-click the row representing an Aggregation Member: • The "Interface Form" on page 113 displays all details about the selected Interface. • The "Layer 2 Connection Form" on page 255 displays all details about the selected Layer 2 Connection.

Layer 2 Connection Form: Registration Tab

The "Layer 2 Connection Form" on page 255 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. **Note:** This value does not change when a node is rediscovered. This is because the Node object is modified, but not created.
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. Note the following: • 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. • 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.

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.

Chassis Redundancy Group Form

Chassis Redundancy Groups are configured to provide redundancy protection against Chassis failure.

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

For information about each tab:

Basic Attributes

Attribute	Description
Name	Name assigned to the Chassis Redundancy Group. NNMi uses the Node Name followed by a slash and then the name that is specific to the Device Vendor:
Status	Overall status for the current Chassis Redundancy Group. NNMi follows the ISO standard for status classification. Possible values are: No Status Normal Disabled Unknown Warning Minor Major Critical **Note:** The icons are displayed only in table views.
Status Last Modified	The date and time when the Status value was last modified.

Chassis Redundancy Group Form: Redundant Components Tab

Chassis Redundancy Groups are configured to provide redundancy protection against Chassis failures.

The "Chassis Redundancy Group Form" above provides details about the selected Chassis Redundancy Group.

For information about each tab:

Redundant Group Member Chassis

Attribute	Description
Redundant Chassis	Table of all of the chassis that are members of this Chassis Redundancy Group. Use this table to access information about each chassis associated with the selected Chassis Redundancy Group. Double-click the row representing a Chassis. The "Chassis Form" on page 193 displays all details about the selected Chassis. **Note:** Only parent Chassis can be members of this group, child Chassis are not permitted to participate in Chassis Redundancy Groups.

Chassis Redundancy Group Form: Incidents Tab

Chassis Redundancy Groups are configured to provide redundancy protection against Chassis failures.

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

For information about each tab:

Incidents Associated with Chassis in this Redundancy Group

Attribute	Description
Incidents	Table of the Incidents associated with the selected Chassis Redundancy Group. 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 Chassis Redundancy Group. Double-click the row representing an Incident. The "Incident Form" on page 437 displays all details about the selected incident. **Tip:** See "Incident Form" on page 437 for more details about the incident attributes that appear in the incident table's column headings.

Chassis Redundancy Group Form: Status Tab

Chassis Redundancy Groups are configured to provide redundancy protection against chassis failures.

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

For information about each tab:

Chassis Redundancy Group Status History Table

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

Chassis Redundancy Group Status History Form

Chassis Redundancy Group Status is derived from SNMP polling results for each Chassis in the Chassis Redundancy Group, as well as any conclusions. For information about how the current Status was determined, see the "Chassis Redundancy Group Form: Conclusions Tab" below. Status reflects the most serious outstanding conclusion. See "Watch Status Colors" on page 406 for more information about possible status values.

Status Attributes

Attribute	Description
Status	Overall status for the current Chassis Redundancy Group. NNMi follows the ISO standard for status classification. Possible values are: No Status Normal (one Active card and one Standby card) Disabled Unknown Warning Minor Major Critical **Note:** The icons are displayed only in table views.
Status Last Modified	Date and time indicating when the Status was last set.

Chassis Redundancy Group Form: Conclusions Tab

Chassis Redundancy Groups are configured to provide redundancy protection against Chassis failures.

The "Chassis Redundancy Group Form" on page 270 provides details about the selected Chassis Redundancy Group.

For information about each tab:

Outstanding Status Conclusion Values

Attribute	Description
Outstanding Status Conclusions	The dynamically generated list of summary statuses for the Chassis Redundancy Group that contributed to the current overall Status of the selected Chassis Redundancy Group. Status is set by the Causal Engine. Each Conclusion listed is outstanding and contributes to the current overall Status. This table is useful for obtaining a quick summary of the problem description for the current Chassis Redundancy Group that led up to the Chassis Redundancy Group's most current Status. The Status value is correlated based on the most critical Conclusions. Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion. The following table describes the possible Conclusions that might appear for a Chassis Redundancy Group object. **Note:** Inter switch links (ISL) are Layer 2 connections that connect chassis. The interfaces in these connections are on the same node, but they are associated with ports on different chassis in a Chassis Redundancy Group. **Note:** A **Y** in the **Incident?** column indicates that the conclusion results in an incident. **Major Status Conclusions** **Conclusion** / **Description** / **Status** / **Incident?** StackWithNoSlave / No Chassis in the Chassis Redundancy Group has a SLAVE State. / Major / Y **Minor Status Conclusions** **Conclusion** / **Description** / **Status** / **Incident?** StackDegraded / NNMi has detected the following conditions in the Chassis Redundancy Group: • One Chassis with a MASTER State • One Chassis with a SLAVE State • Other Chassis in the group are not in SLAVE State / Minor / Y ISLAggregatorLinkDown / (*NNMi Advanced*) At least one of the / Minor / N

Outstanding Status Conclusion Values, continued

Attribute	Description
	Conclusion / **Description** / **Status** / **Incident?** Inter Switch Links between Chassis in the Chassis Redundancy Group is down. See "Aggregator Connection Down (NNMi Advanced)" on page 496 for more information.

Warning Status Conclusions

Conclusion	Description	Status	Incident?
ISLAggregatorLinkDegraded	(*NNMi Advanced*) At least one of the Inter Switch Links between Chassis in the Chassis Redundancy Group is degraded. See "Aggregator Connection Degraded (NNMi Advanced)" on page 495 for more information.	Warning	N

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	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: **Card Redundancy Group Naming Conventions** **Device Vendor** / **Naming Convention** Cisco / <*nodename*>/Supervisor Engine Group **Note:** Only cards classified as Management Modules are

Basic Attributes, continued

Attribute	Description
	Card Redundancy Group Naming Conventions, continued considered for Card Redundancy Groups. HPE ProCurve: <*nodename*>/Management Module Group **Note:** Only cards classified as Management Modules are considered for Card Redundancy Groups.
Status	Overall status for the current Card Redundancy Group. NNMi follows the ISO standard for status classification. Possible values are: No Status Normal Disabled Unknown Warning Minor Major Critical **Note:** The icons are displayed only in table views.
Status Last Modified	The date and time when the Status value was last modified.

Card Redundancy Group Form: Redundant Components 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	Table of all of the Physical Component: 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. Double-click the row representing a Card. The "Card Form" on page 211 displays all details about the selected Card. **Note:** Only parent cards can be members of this group, child cards are not permitted to participate in Card Redundancy Groups.

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 page 274 provides details about the selected Card Redundancy Group.

For information about each tab:

Incidents Associated with Cards in this Redundancy Group

Attribute	Description
Incidents	Table of the Incidents associated with the selected Card Redundancy Group. 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. Double-click the row representing an Incident. The "Incident Form" on page 437 displays all details about the selected incident. **Tip:** See "Incident Form" on page 437 for more details about the incident attributes that appear in the incident table's column headings.

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 274 provides details about the selected Card Redundancy Group.

For information about each tab:

Card Redundancy Group Status History Table

Attribute	Description
Status History	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. Double-click the row representing a Status History. The "Card Redundancy Group Status History Form" below displays all details about the selected Status.

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" below. Status reflects the most serious outstanding conclusion. See "Watch Status Colors" on page 406 for more information about possible status values.

Status Attributes

Attribute	Description
Status	Overall status for the current Card Redundancy Group. NNMi follows the ISO standard for status classification. Possible values are: No Status Normal (one Active card and one Standby card) Disabled Unknown Warning Minor Major Critical **Note:** The icons are displayed only in table views.
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 274 provides details about the selected Card Redundancy Group.

For information about each tab:

Outstanding Status Conclusion Values

Attribute	Description
Outstanding Status Conclusions	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. Each Conclusion listed is outstanding and contributes to the current overall Status. 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. The Status value is correlated based on the most critical Conclusions. Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion. The following table describes the possible Conclusions that might appear for a Card Redundancy Group object. **Note:** A **Y** in the **Incident?** column indicates that the conclusion results in an incident.

Critical Status Conclusions

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: • One card, or both the Primary and Secondary Cards, are down. • NNMi has identified only Secondary cards (for example Standby cards) in the group. • Communication between cards in the group is malfunctioning.	Critical	Y

Warning Status Conclusions

Conclusion	Description	Status	Incident?
CrgNoSecondary	A Card Redundancy Group does not have a secondary member. Neither card has a cardStandbyStatus equal to Standby. A	Warning	Y

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	properly functioning Card Redundancy Group should have one operational Primary Card and one operational Secondary Card.		

Unknown Status Conclusions

Conclusion	Description	Status	Incident?
CrgUnmanagable	The SNMP Agent on the node hosting the Card Redundancy Group is not responding to SNMP queries.	Unknown	N

Normal Status Conclusions

Conclusion	Description	Status	Incident?
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
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 *Active* or VRRP *Master*).
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 See "Watch Status Colors" on page 406 for more information about Severity values. **Note:** 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 (**VRRP**[1]) or Hot Standby Router Protocol (**HSRP**[2]) .
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" on page 402

[1]Virtual Router Redundancy Protocol
[2]Hot Standby Router Protocol

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

The "Router Redundancy Group Form (NNMi Advanced)" on page 279 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 "Router Redundancy Member Form (NNMi Advanced)" below displays all details about the selected Router Redundancy Member.

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	Name of the selected router and its associated interface that is a member of the current Router Redundancy Group. **Note:** NNMi determines this Name value. The name includes the fully-qualified DNS hostname assigned to the router and the Name attribute value that NNMi assigned to the interface. This name appears in the following format:

Basics Attributes, continued

Attribute	Description
	<fully qualified hostname assigned to the router>[*Interface Name*:*group_number*] For example: `HSRPRouter1.abc.example.com[Se1/1:1]` See "Node Form" on page 65 for more information about node names. See "Interface Form" on page 113 for more information about interface names.
Primary IP	The IP Address used to exchange messages between routers in the Router Redundancy Group.
Is Owner	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 287 for more information. If the selected router uses a Router Redundancy Protocol that does not support virtual addresses, the value is set to `false`.
Priority	The configured protocol-specific number that indicates the current rank of the Router Redundancy Member.
Redundancy Interface	The interface that is being used by the router to participate in the Router Redundancy Group. To find out more information about this Interface: Click the Lookup icon and choose one of the following options: • Show Analysis to view the Analysis Pane information for the selected interface. (See "Use the Analysis Pane " on page 482 for more information about the Analysis Pane.) • Open to open the Interface form.
Hosted on Node	Name attribute value from the "Node Form" on page 65 of the selected router (the Router Redundancy Group member). To find out more information about the Node: Click the Lookup icon and choose one of the following options: • Show Analysis to view the Analysis Pane information for the selected interface. (See "Use the Analysis Pane " on page 482 for more information about the Analysis Pane.) • Open to open the Node form.
Redundancy Group	Name of the Router Redundancy Group to which the Router Redundancy Member belongs. To find out more information about the Router Redundancy Group: Click the Lookup icon and choose one of the following options: • Show Analysis to view the Analysis Pane information for the selected interface. (See "Use the Analysis Pane " on page 482 for more information about the Analysis Pane.) • Open to open the Router Redundancy Group form.
Current	State of the Router Redundancy Member. State values are protocol-specific. For example:

Basics Attributes, continued

Attribute	Description
State	• **Hot Standby Router Protocol (HSRP) States:** click here. **Active** - Indicates the router is forwarding packets that are sent to the router redundancy group. **Standby** - Indicates the router is a candidate to become the next active router. **Initial** - Indicates **HSRP**[1] is not running. This state occurs when an interface first comes up. **Learn** - 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. **Listen** - 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. **Speak** - 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. • **Virtual Router Redundancy Protocol (VRRP) States:** click here. **Master** - Indicates the router is forwarding packets that are sent to the router redundancy group. **Backup** - Indicates the router is a candidate to become the next master router. **Initialize** - Indicates the router is not running VRRP protocol. This state occurs when an interface first comes up. The following values indicate NNMi could not gather the required data: **Agent Error** – Indicates an error was returned in response to the query. **No Polling Policy** - No polling policy exists for this monitored attribute. **Not Polled** - 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. **Not Provided** — The device does not support providing information for this monitored attribute. **Unavailable** - The agent responded with a value outside the range of possible values or returned a null value. **Unset** – Currently not used by NNMi. **Other** – The SNMP agent responded with a value for the MIB variable used to determine the Router Redundancy Member State that is not recognized.

[1]Hot Standby Router Protocol

Basics Attributes, continued

Attribute	Description
Previous State	The previous State of the Router Redundancy Member. State values are protocol-specific. For examples, see Current State.
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 281 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	Name of the selected router and its associated interface that is a member of the current Router Redundancy Group. **Note:** NNMi determines this Name value. The name includes the fully-qualified DNS hostname assigned to the router and the Name attribute value that NNMi assigned to the interface. This name appears in the following format: <*fully qualified hostname assigned to the router*>[*Interface Name*] For example: `HSRPRouter1.abc.example.com[Se1/1]` **Note:** NNMi determines this Name value. See "Node Form" on page 65 for more information about node names. See "Interface Form" on page 113 for more information about interface names.
Track Priority	Number NNMi uses to rank the tracked object whenever a Current State change occurs. NNMi uses this number indirectly in the calculation to determine the next Primary member of the Router Redundancy Group. 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

Tracked Objects Table, continued

Attribute	Description
	numbers, the member with the highest Priority value becomes the new Primary router in the Router Redundancy Group. 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: • The Track Priority (20) is subtracted from its member Priority (250-20=230). • The new member Priority (230) is then compared to the Priority value of the other members in the Router Redundancy Group. • 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).
State Last Modified	The date and time when the State value was last modified.

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	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 . **Note:** NNMi determines this Name value. The name includes the fully-qualified DNS hostname assigned to the router and the Name attribute value that NNMi assigned to the interface. This name appears in the following format: <*fully qualified hostname assigned to the router*>[*Interface Name*] For example: `HSRPRouter1.abc.example.com[Se1/1]` See "Node Form" on page 65 for more information about node names. See "Interface Form" on page 113 for more information about interface names. To find out more information about this interface: Click the Lookup icon and choose one of the following options: • Show Analysis to view the Analysis Pane information for the selected Tracked Object.

Basics Attributes, continued

Attribute	Description
	(See "Use the Analysis Pane " on page 482 for more information about the Analysis Pane. • Open to open the Interface form.
Track Priority	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. 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. 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: • The Track Priority (20) is subtracted from its member Priority (250-20=230). • The new member Priority (230) is then compared to the Priority value of the other members in the Router Redundancy Group. • 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.
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 279 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 "Virtual IP Addresses Form (NNMi Advanced)" on the next page 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 279 provides details about the selected Router Redundancy Group.

For information about each tab:

Incidents Associated with this Router Redundancy Group

Attribute	Description
Incidents	Table of the Incidents associated with the selected Router Redundancy Group. These Incidents are sorted by creation time so that you can view the Incidents in chronological order. Use this table to determine which Incidents are still open for the selected Router Redundancy Group. Double-click the row representing an Incident. The "Incident Form" on page 437 displays all details about the selected incident. **Tip:** See "Incident Form" on page 437 for more details about the incident attributes that appear in the incident table's column headings.

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

The "Router Redundancy Group Form (NNMi Advanced)" on page 279 provides details about the selected Router Redundancy Group.

For information about each tab:

Router Redundancy Group Status History Table

Attribute	Description
Status History	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. 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.

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 406 for more information about possible status values.

Status Attributes

Attribute	Description
Status	Overall status for the current Router Redundancy Group. NNMi follows the ISO standard for status classification. Possible values are: No Status Normal Disabled Unknown Warning Minor Major Critical **Note:** The icons are displayed only in table views.
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 279 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	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. Each Conclusion listed is outstanding and contributes to the current overall Status. 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. The Status value is correlated based on the most critical Conclusions. Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion. The following table describes the possible Conclusions that might appear for a Router Redundancy object. **Note:** A **Y** in the **Incident?** column indicates that the Conclusion results in an incident. **Critical Status Conclusions** **Major Status Conclusions**

Critical Status Conclusions

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: • Too many routers are down. • Protocol-specific communication between routers in the group is malfunctioning.	Critical	Y

Outstanding Status Conclusion Values, continued

Attribute	Description

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

Minor Status Conclusions

Conclusion	Description	Status	Incident?
RrgMultipleSecondary	Indicates that more than one secondary device is identified in a Router Redundancy Group (for example, HSRP Standby). **Note:** 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. Typically, the protocol-specific communication between routers in the group is malfunctioning.	Minor	Y
RrgNoSecondary	Indicates that zero routers in a Router Redundancy Group are designated as Secondary (for example, no router reporting 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 a single Primary device has been identified.	Minor	Y

Warning Status Conclusions

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
RrgGroupContainsUnmanagedMember	At least one, but not all SNMP Agents, associated with the member interfaces are not responding to SNMP queries or are not polled.	Warning	N
RrgDegraded	This incident occurs only in Router Redundancy Groups with more than two members. This incident typically indicates the following: • The Router Redundancy Group has a Primary and Secondary device. • The remaining devices in the group are not in an expected protocol-specific state (for example, zero routers reporting HSRP Listen state). • Typically, the protocol-specific communication between routers is malfunctioning. However, the group is routing packets properly.	Warning	Y

Unknown Status Conclusions

Conclusion	Description	Status	Incident?
RrgGroupAllMembersUnmanaged	The SNMP Agent associated with all Router	Unknown	N

Outstanding Status Conclusion Values, continued

Attribute	Description

Conclusion	Description	Status	Incident?
	Redundancy Group member's interfaces are not responding to SNMP queries or are not polled.		

Normal Status Conclusions

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 279 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. **Note:** This value does not change when a node is rediscovered. This is because the Node object is modified, but not created.
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. Note the following: • 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. • 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.

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	*NNMi Administrators only*. If disabled ☐, NNMi does not calculate the Status for this Node Group. NNMi sets the Node Group Status value to No Status. If enabled ☑, NNMi calculates the Node Group Status according to the Status Configuration settings. See "Configure Node Group Status" for more information.
Status	Overall status for the specified node group. NNMi follows the ISO standard for status

Node Group Basic Settings, continued

Attribute	Description
	classification. See the "Node Group Form: Status Tab" on page 300 for more information.
Add to View Filter List	*NNMi Administrators only*. If disabled ☐, this node group does not appear in any node group filter lists for node, interface, IP address, and incident views. If enabled ☑, this node group is available as a filter for all node, interface, IP address, and incident views.
Notes	*Optional*. If your role permits, enter any information that might be useful to you and your team. Type a maximum of 1024 characters. Alpha-numeric, spaces, and special characters (~ ! @ # $ % ^ & * ( ) _+ -) are permitted.

NNM iSPI Performance

Attribute	Description
Add to Filter List	*NNMi Administrators only*. Using this feature is entirely optional. The NNM iSPI Performance software, such as NNM iSPI Performance for Metrics or NNM iSPI Performance for Traffic, can monitor your network without any exported filter. 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. If disabled ☐, this group is not available as a filter in NNM iSPI Performance reports. If enabled ☑, this group appears in the Optional Filters selection panel of the NNM iSPI Performance reports. Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics) -- click here for more information. Requires HPE Network Node Manager iSPI Performance for Traffic Software (NNM iSPI Performance for Traffic) -- click here for more information.

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.

Note: The "Node Group Form" on page 293 provides details about the selected node group.

For information about each tab:

Device-Characteristic Filters Table

Attribute	Description
Device Filter	Table view of the device category, vendor, product family, or product model filters associated with the selected node group. Double-click the row representing the node that has the "Node Device Filter Form (NNMi Administrators only)" below you want to see.

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	*Optional:* A particular category of devices. The drop-down list displays all available choices.
Device Vendor	*Optional:* A particular vendor. The drop-down list displays all available choices.
Device Family	*Optional:* A particular family of devices. The drop-down list displays all available choices.

Device Attribute Filters Table , continued

Attribute	Description
Device Category	*Optional:* A particular category of devices. The drop-down list displays all available choices.
Device Profile	*Optional:* The text string for Device Model from the Device Profile. **Tip:** According to industry standards (RFC 1213, MIB-II), each combination of vendor, category, and model is assigned a unique SNMP system object ID number (**sysObjectID**). 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). If your role permits, click the Lookup icon and select one of the options from the drop-down menu: • Show Analysis to view Analysis Pane information for the currently selected Device Profile. (See "Use the Analysis Pane " on page 482 for more information about the Analysis Pane.) • Quick Find to view and select from the list of all existing Device Profiles. • Open to display the details of the currently selected Device Profile. • New to create a new Device Profile definition.

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.

Note: The "Node Group Form" on page 293 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 293 provides details about the selected node group.

For information about each tab:

Specific-Device Filters Table

Attribute	Description
Node Hostname	Table view of the *case-sensitive* 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)" above.

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

Tip: 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 "Custom Node Attribute Samples" on page 88 and Add Custom Attributes to Multiple Objects for more information.

Specific Node Group Member

Attribute	Description
Node Hostname	The current value of the *fully-qualified, case-sensitive* Hostname attribute as it appears on the Node form. 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. • 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). When the NNMi administrator chooses **Enable SNMP Address Rediscovery** ☑ in the

Specific Node Group Member, continued

Attribute	Description
	Communication Configuration: • If the SNMP Agent does not respond, NNMi checks for another Management Address to request the Hostname, and the Hostname could change. • If the SNMP Agent associated with the node changes, the Management Address and Hostname could change. When the NNMi administrator disables **Enable SNMP Address Rediscovery** ☐ in the Communication Configuration, when the current management address (SNMP agent) becomes unreachable, NNMi does not check for other potential management addresses. • 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. **Note:** NNMi administrators can use NNMi property file settings to change the way NNMi determines Hostname values: • `nms-topology.properties` 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 *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`. • `nms-disco.properties` 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 *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`. See "Access Node Details" on page 409 and Access More Details (Forms and Analysis Pane) for a description of the ways to verify node details.

Node Group Form: Child Node Groups Tab (*NNMi Administrators only*)

The "Node Group Form" on page 293 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)" below.

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 368

"Navigating within a Node Group Map" on page 370

"Position Nodes on a Node Group Map" on page 372

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

Basics Attributes, continued

Attribute	Description
Child Node Group	Indicates the name of a Node Group that is below the current Node Group in the hierarchical order. For example, **Colorado** could be a Child Node Group to a Node Group named **United States**. **Note:** This attribute appears as the **Name** column in the **Child Node Groups** table view.

	If disabled, a single object represents a Child Node Group on the Node Group Map.
	
	Note the following:
	• If the current Node Group has one or more Child Node Groups, each Child Node Group is also displayed. Child Node Groups are indicated using a hexagon as shown below:
	
	• 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:
	  • If the Child Node Group has the **Expand Child in Parent Node Group Map** attribute disabled, the Child Node Group appears as a hexagon.
	  • If any Child Node Group has the **Expand Child in Parent Node Group Map** attribute enabled, NNMi displays each of the nodes in that Child Node Group.
	
	Note: This attribute appears in the **Expand** column in the **Child Node Groups** table view.

Related Topics

"Node Group Maps" on page 368

"Position Nodes on a Node Group Map" on page 372

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.

When propagating Node Group status, NNMi uses the following severity order (from lowest to highest):

No Status

Normal

Unknown

Warning

Minor

Major

Critical

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 293 provides details about the selected Node Group.

For information about each tab:

Status Attributes

Attribute	Description
Status	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: • Propagating the Most Severe Status (NNMi default setting) • Configuring percentage thresholds Possible status values are as follows. See "Watch Status Colors" on page 406 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):

Status Attributes , continued

Attribute	Description
	No Status **Unknown** **Minor** **Normal** **Warning** **Major** **Critical**
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 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 ☐, this interface group does not appear in any interface group filter lists for interface and IP address views. If enabled ☑, this interface group is a filter for all interface and IP address views.
Node Group	*Optional*. 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 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	*Optional*. If your role permits, enter any information that might be useful to you and your team. Type a maximum of 1024 characters. Alpha-numeric, spaces, and special characters (~ ! @ # $ % ^ & * ( ) _+ -) are permitted.

NNM iSPI Performance

Attribute	Description
Add to Filter List	*NNMi Administrators only*. Using this feature is entirely optional. The NNM iSPI Performance software, such as NNM iSPI Performance for Metrics or NNM iSPI Performance for Traffic, can monitor your network without any exported filter. 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. If disabled ☐, this group is not available as a filter in NNM iSPI Performance reports. If enabled ☑, this group appears in the Optional Filters selection panel of the NNM iSPI Performance reports. Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics) -- click here for more information. Requires HPE Network Node Manager iSPI Performance for Traffic Software (NNM iSPI Performance for Traffic) -- click here for more information.

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 page 302 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: `http://www.iana.org/assignments/ianaiftype-mib`)

ifType (Interface Type) Form

Displays information about the `IANA ifType-MIB` file's `ifType` variable value assigned to the selected type of interface (make and model).

For more information, see: `http://www.iana.org/assignments/ianaiftype-mib`

To access the ifType form, do one of the following:

- Open any "Interface Form: General Tab" on page 118.
- Open any "Interface Group Form: ifType Filters Tab" on the previous page.

Interface Type Definition

Attribute	Description
ifType	`IANA ifType-MIB` file's text string assigned to this kind of interface.
Number	`IANA ifType-MIB` file's unique number assigned to this kind of interface.
Description	A description of this type of interface. Maximum of 2048 characters. Alpha-numeric, spaces, and special characters (~ ! @ # $ % ^ & * ( ) _+ -) are permitted. *Optional*. NNMi Administrators can navigate to the **Configuration → MIBs → ifTypes** view and modify the description text to provide useful information to your team.

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.

Note: The "Interface Group Form" on page 302 provides details about the selected Interface Group.

For information about each tab:

MPLS WAN Cloud (RAMS) Form (*NNMi Advanced*)

(*NNMi Advanced*, plus *HPE Route Analytics Management System (RAMS) for MPLS WAN*) 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 Name	The name assigned to the discovered MPLS WAN Cloud.
AS Number	The **Autonomous System**[1] 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 389

MPLS WAN Cloud (RAMS) Form: MPLS WAN Connections Tab (*NNMi Advanced*)

(*NNMi Advanced*, plus *HPE Route Analytics Management System (RAMS) for MPLS WAN*) 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**[2]) router. The possible values are: No Status Normal Disabled Unknown Warning Minor Major

[1]An Autonomous System (AS) is a collection of connected Internet Protocol (IP) routing prefixes that present a common, clearly defined Border Gateway Protocol (BPG) routing policy to the Internet by having an officially registered Autonomous System Number (ASN).
[2]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 desination.

Basic Attributes, continued

Attributes	Description
	Critical
CE Name	The name assigned to the CE router.
CE Interface	Interface of the CE router participating in the MPLS WAN Cloud.
CE Address	The IP address of the CE router.
PE Address	The IP address of the Provider Edge (**PE**[1]) router.
Protocol	The routing protocol used between the CE and the PE router.

Related Topics:

"MPLS WAN Cloud Map (NNMi Advanced)" on page 389

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	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). Click the Lookup icon and select Show Analysis or Open to display more information about the node.
Active State	The Active State for the associated Custom Collect Policy. Possible values are described below: **Active** - Indicates the Custom Poller Policy is in use.

[1]Provider Edge router. The Internet Service Provider's router that receives your data on the path to your data's final desination. The Customer Edge (CE) router in your network connects to this PE.

Basic Attributes, continued

Attribute	Description
	Note: At the time the Active State attribute is set to **Active**, NNMi applies the Custom Poller Policy to the nodes in the specified Node Group to determine which instances should be polled. **Inactive** - Indicates the Custom Poller Policy is not in use. NNMi removes all Polled Instances associated with the Policy. **Suspended** - Indicates someone on your team changed this Custom Poller Policy's *Active State* to Suspended, or the NNMi administrator disabled Custom Poller in the *Global Control* settings of **Configuration** workspace, **Custom Poller Configuration** form. NNMi suspends polling and retains the most recent State value from before the Policy was suspended.
Status	The most severe State value returned from the Custom Poller Polled Instances for this Custom Node Collection. Possible values are: Normal Warning Minor Major Critical
Policy	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. 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.
Discovery State	Indicates the progress toward collecting data associated with this Polled Instance (discovery using the MIB Expression objects for which you are collecting information). Possible values include: **Created** - NNMi has not yet discovered any data for this new Polled Instance. **In progress** - NNMi is currently collecting data for this Polled Instance. **Completed** - NNMi gathered the data associated with this Polled Instance and placed it in the NNMi database. **Unresponsive** - The SNMP agent did not respond when NNMi attempted to gather the data associated with this Polled Instance. **Failed** - NNMi is unable to gather the data associated with this Polled Instance. Look in the Discovery State Information field for details.

Basic Attributes, continued

Attribute	Description
Discovery State Last Modified	The date and time when the Discovery State value was last modified.
Discovery State Information	Indicates any problems contributing to the Discovery State calculation.

Related Topics

About Custom Poller

Custom Node Collections Form: Incidents Tab

The "Custom Node Collections Form" on page 307 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 437 displays all details about the selected incident.

Custom Node Collections Form: Status Tab

The "Custom Node Collections Form" on page 307 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: Normal Warning

Overall Status, continued

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

Custom Node Collections Form: Conclusions Tab

The "Custom Node Collections Form" on page 307 provides details about the selected Custom Node Collection.

For information about each tab:

Outstanding Status Conclusion Values

Attribute	Description
Outstanding Status Conclusions	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. Each Conclusion listed is still outstanding and applies to the current overall Status. This view is useful for obtaining a quick summary of the Status and problem description that led up to the Custom Node Collection's most current Status. The Status value is correlated based on the most critical outstanding Conclusions. Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion. The following table describes the possible Conclusions that might appear for a Custom Node Collection object. **Note:** A **Y** in the **Incident?** column indicates that the Conclusion results in an incident.

Outstanding Status Conclusion Values, continued

Attribute	Description
	Critical Status Conclusions **Conclusion** | **Description** | **Status** | **Incident?** CustomPollCritical | A Custom Polled Instance associated with the Custom Poller Collection is in a Critical State. | Critical | Y **Major Status Conclusions** **Conclusion** | **Description** | **Status** | **Incident?** CustomPollMajor | A Custom Polled Instance associated with the Custom Poller Collection is in a Major State. | Major | Y **Minor Status Conclusions** **Conclusion** | **Description** | **Status** | **Incident?** CustomPollMinor | A Custom Polled Instance associated with the Custom Poller Collection is in a Minor State. | Minor | Y **Warning Status Conclusions** **Conclusion** | **Description** | **Status** | **Incident?** CustomPollWarning | A Custom Polled Instance associated with the Custom Poller Collection is in a Warning State. | Warning | Y **Normal Status Conclusions** **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

The "Custom Node Collections Form" on page 307 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	Information about Custom Poller Policy information being collected. This table is useful for obtaining a quick summary. Double-click the row representing a Polled Instance. The "Custom Polled Instance Form" below displays all details about the selected Polled Instance.

Custom Polled Instance Form

The **Custom Polled Instance**[1] 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.

[1] A Custom Polled Instance represents the results of a MIB variable when it is evaluated against a node. The first time a MIB variable 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.

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.

Basic Attributes

Attribute	Description
Node	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). Click the Lookup icon and select Show Analysis or Open to display more information about the topology node.
MIB Instance	This attribute contains the multiple filtered instances for the MIB Expression. Each instance value identifies a row in the MIB table. **Note:** 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.
Filter Value	The instance of a MIB Variable value after the MIB Filter is applied.
Display Attribute	The MIB Variable that contains the values NNMi displays when generating Custom Polled Instance or Line Graph results. **Note:** The NNMi administrator selects this **Display Variable** when configuring the MIB Expression for a Custom Poller Collection.
Active State	Specifies whether a Custom Poller Policy is enabled.
Custom Node Collection	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. Click the Lookup icon and select Show Analysis or Open to display more information about the Custom Node Collection. See "Custom Node Collections Form" on page 307 for more information.
MIB Variable	The MIB Variable that is associated with this Custom Poller Instance. See Specify the MIB Variable Information for a Custom Poller Collection for more information.
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.

Basic Attributes, continued

Attribute	Description
Custom Poller Collection	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. Click the Lookup icon and select Show Analysis or Open to display more information about the Custom Poller Collection. See "Custom Polled Collection Form" on page 317 for more information.
Status	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: Normal Warning Minor Major Critical Status reflects the most serious outstanding conclusion. See "Watch Status Colors" on page 406 for more information about possible status values. **Note:** The icons are displayed only in table views
State	The State of the Custom Polled Instance as determined by any Thresholds (High State / Low State 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. Possible State values for a *Polled Instance* (Threshold = High State/Low State; or Comparison Map = State Mapping) are: Normal Warning Minor Major Critical **Note:** The most severe Threshold High State or Low State value or Comparison Map *State Mapping* value returned from the Polled Instances for a Custom Node Collection becomes the Custom Node Collection Status.
Last State	The value from the MIB Expression that most recently caused the State to change.

Basic Attributes, continued

Attribute	Description
Change Value	**Note:** A value of **null** 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.

Custom Polled Instance Form: Incidents Tab

Tip: The "Custom Polled Instance Form" on page 312 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 437 displays all details about the selected incident.

Custom Polled Instance Form: Status Tab

The "Custom Polled Instance Form" on page 312 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:

Overall Status, continued

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

Custom Polled Instance Form: Conclusions Tab

The "Custom Polled Instance Form" on page 312 provides details about the selected Custom Polled Instance.

For information about each tab:

Outstanding Conclusions Table

Attribute	Description
Outstanding Status Conclusions	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. Each Conclusion listed is still outstanding and applies to the current overall Status. This view is useful for obtaining a quick summary of the Status and problem description that led up to the Custom Polled Instances most current Status. The Status value is correlated based on the most critical outstanding Conclusions. Double-click the row representing a Conclusion. The Conclusion form displays all details about the selected Conclusion. The following table describes the possible Conclusions that might appear for a Custom Polled Instance object.

Outstanding Conclusions Table, continued

Attribute	Description

Note: A **Y** in the **Incident?** column indicates that the Conclusion can result in an incident. An NNMi administrator can configure whether incidents are generated. See Configure Basic Settings for a Custom Poller Collection for more information.

Critical Status Conclusions

Conclusion	Description	Status	Incident?
CustomPolledInstanceCritical	A Custom Polled Instance is in a Critical State.	Critical	Y

Major Status Conclusions

Conclusion	Description	Status	Incident?
CustomPolledInstanceMajor	A Custom Polled Instance is in a Major State.	Major	Y

Minor Status Conclusions

Conclusion	Description	Status	Incident?
CustomPolledInstanceMinor	A Custom Polled Instance is in a Minor State.	Minor	Y

Warning Status Conclusions

Conclusion	Description	Status	Incident?
CustomPolledInstanceWarning	A Custom Polled Instance is in a Warning State.	Warning	Y

Normal Status Conclusions

Conclusion	Description	Status	Incident?
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: • when a threshold is crossed • when a polled MIB value causes the Custom Polled Collection's State to be other than **Normal**
Export Custom Poller Collection	If enabled ☑, NNMi exports the Custom Poller Collection to a comma-separated values (CSV) file If disabled ☐, NNMi does not export the Custom Poller Collection information.
Compress Export File	If enabled ☑, NNMi exports the Custom Poller Collection in compressed format and appends .gz to the .csv file suffix. If disabled ☐, 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: • **Count** threshold based on the number of occurrences specified before the threshold is reached. • **Time** threshold based on the duration of time specified before the threshold is reached.
High State	Possible values are: • Normal • Warning • Minor • Major • Critical
High Value	The value that above which becomes a threshold situation. Use one of the following: • Designate a percentage between 0.00 and 100.00. For special situations, the following values can be used: • 0.000000000000001 (or 1E-15 in Scientific Notation) for the smallest value greater than zero. • 99.99999999999999 for the highest value less than one hundred. • Designate any appropriate integer value (for example, a Management Address ICMP Response Time of 0 or greater milliseconds). The High Value must be greater than or equal to the designated Low Value. **Note:** If you use the highest possible value, the threshold is disabled because it cannot be *crossed*.
High Value Rearm	The High Value Rearm designates the lower boundary of the High Threshold *range of values*.
Threshold Setting Type = Count:	
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.
Threshold Setting Type = Time (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: • Normal • Warning • Minor • Major • Critical
Low Value	The value that below which becomes a threshold situation. Use one of the following: • Designate a percentage between 0.00 and 100.00. For special situations, the following values can be used: • 0.000000000000001 (or 1E-15 in Scientific Notation) for the smallest value greater than zero. • 99.99999999999999 for the highest value less than one hundred. • Designate any appropriate integer value (for example, a Management Address ICMP Response Time of 0 or greater milliseconds). The Low Value must be less than or equal to the designated High Value. **Note:** If you use the minimum possible value, the Low threshold is disabled because it cannot be *crossed*.
Low Value Rearm	The Low Value Rearm designates the upper boundary of the Low Threshold *range of values*.
Threshold Setting Type = Count:	
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.
Threshold Setting Type = Time (setting both of these to zero disables the Low Threshold):	
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. **Note:** 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.
Comparison Operator	Operator used to evaluate the polled value and subsequently determine its State. For example, the < (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.
Comparison Value	The value to which the polled value is compared.
State Mapping	The State to assign to the Custom Poller Polled Instance when the polled value meets the comparison criteria. For example, each time the value **3** (warning) is returned when NNMi polls hrDeviceStatus, you can specify that you want NNMi to change the State of the Polled Instance to **Warning**. Possible State values for a *Polled Instance* (Threshold = High State/Low State; or Comparison Map = State Mapping) are: Normal Warning Minor Major Critical

Chapter 6: Scheduling Outages for Nodes or Node Groups

NNMi Administrators and Level-2 Operators can configure Scheduled Outages. During the specified Scheduled Outage time period, NNMi changes the Node Management Mode to **Out-of-Service** and suspends any Discovery or Monitoring of that Node. When the specified time period ends, NNMi changes the Node Management Mode to **Managed**, gathers current information, and updates the Node data.

Prerequisite: "Understand the Effects of Setting the Management Mode to Not Managed or Out of Service" on page 589

For a list of all past, present, and future Scheduled Node Outages, see the "Scheduled Node Outages View" on page 586.

(*NNMi Advanced*) If the Global Network Management feature is enabled and you are signed into a Global Manager:

- If the Node is managed by the Global Manager = applying **Actions** → **Management Mode** → **Schedule Node Outage** modifies the Node object in the Global Manager's database. The information is not sent to any Regional Manager.
- If the Node is managed by a Regional Manager = you must first use **Actions** → **Open from Regional Manager** prior to scheduling the outage on Regional Manager that is responsible for this Node. Any resulting change in a Node's Management Mode is communicated to the Global Manager.

  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 *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.

To configure a past, present, or future scheduled outage using a Node view:

1. Navigate to the Node view of interest.
2. Do one of the following:
   - Select the table row or map icon that represents the Node of interest.
   - Use Ctrl-click to select multiple Nodes.
3. Select **Actions** → **Management Mode** → **Schedule Node Outage** in the main toolbar.

   Tip: You can also right-click any object in a table or map view to access the items available within the **Actions** menu.
4. Specify your choices in the Schedule Node Outage dialog. See Scheduled Node Outage Attributes in the table below.
5. Save your settings:

- If the Scheduled Outage is in the future, click the **Schedule Outage** button to apply your changes.
- If making a record of a Scheduled Outage in the past, click the **Record a Past Outage** button to apply your changes.

To configure a past, present, or future scheduled outage using a Node Group view:

1. Navigate to the Node Group view of interest.
2. Do one of the following:
   - Select the table row or map icon that represents the Node Group of interest.
   - Use Ctrl-click to select multiple Node Groups.
3. Select **Actions** → **Management Mode** → **Schedule Group Members Outage** in the main toolbar.

   Tip: You can also right-click any object in a table or map view to access the items available within the **Actions** menu.
4. Specify your choices in the Schedule Node Outage dialog. See Scheduled Node Outage Attributes in the table below.
5. Save your settings:
   - If the Scheduled Outage is in the future, click the **Scheduled Outage** button to apply your changes.
   - If making a record of a Scheduled Outage in the past, click the **Record a Past Outage** button to apply your changes.

To configure a past, present, or future scheduled outage using an Incidents view:

1. Navigate to the Incident view of interest.
2. Do one of the following:
   - Select one Incident.
   - Use Ctrl-click to select multiple Incidents.
3. Select **Actions** → **Node Actions** → **Management Mode** → **Schedule Node Outage** in the main toolbar.

   Tip: You can also right-click any object in a table or map view to access the items available within the **Actions** menu.
4. Specify your choices in the Schedule Node Outage dialog. See Scheduled Node Outage Attributes in the table below.
5. Save your settings:
   - If the Scheduled Outage is in the future, click the **Scheduled Outage** button to apply your changes.
   - If making a record of a Scheduled Outage in the past, click the **Record a Past Outage** button to apply your changes.

Tip: For the command line method of configuring a Scheduled Node Outage, see the nnmscheduledoutage.ovpl Reference Page.

Scheduled Node Outage Attributes

Attribute		Description
Enabled		☑ - Indicates that at the scheduled time, NNMi will run this Scheduled Outage configuration. ☐ - Indicates that at the scheduled time, NNMi will skip this Scheduled Outage configuration.
Name		Type a maximum of 50 characters. Alpha-numeric, spaces, and special characters (~ ! @ # $ % ^ & * ( ) _+ -) are permitted. **Tip:** *Optional* best practice, choose a name identifying the Scheduled Outage that is unique. The name can communicate the purpose of the Scheduled Outage to your team.
Description		Communicate with your team by providing a description of this scheduled outage. Maximum length is 2,000 characters: alpha-numeric, spaces, and special characters (~ ! @ # $ % ^ & * ( ) _+ -
Start	Date	Select the date from the calendar indicating when NNMi will run this Scheduled Outage.
	Time	Type or select the time from the drop-down indicating when NNMi will run this Scheduled Outage.
End	Date	Select the date from the calendar indicating when NNMi will end this Scheduled Outage.
	Time	Type or select the time from the drop-down indicating when NNMi will end this Scheduled Outage.
Time Zone	Use Server Time Zone	☑ - Indicates that the NNMi server's Time Zone determines this Scheduled Outage configuration's start/stop time. ☐ - Indicates that the NNMi administrator prefers to designate a specific time zone for the start/stop time (see the Specify Time Zone attribute).
	Specify Time Zone	Use the drop-down list to select a Time Zone for this Scheduled Outage configuration (default is the NNMi server's time zone). Some time zones have multiple industry-standard name choices, all appear in the drop-down list. To make NNMi automatically default to the one your team uses, see *HPE Network Node Manager i Software Deployment Reference,*"NNMi Console" chapter. **Tip:** The list of valid Java Time Zones changes over time. To check NNMi's

Scheduled Node Outage Attributes, continued

Attribute		Description
		current Java Time Zone version number, on the server where NNMi is installed, use the following command line tool (see About Environment Variables for more information): **Windows:** *%NnmInstallDir%*\jdk\hpsw\bin\java –version **Linux:** *$NnmInstallDir*/jdk/hpsw/bin/java –version
List of Nodes	Hostname	Use ✱ to add Nodes to this Scheduled Outage configuration. Use 🗑 to remove Nodes from this Scheduled Outage configuration.
	Time Zone	Displays the configured Time Zone if other than the NNMi Server Time Zone. The NNMi administrator creates a Custom Attribute to populate this column. For details, see "Custom Node Attributes Form" on page 87. **Note:** If you don't see a Time Zone setting for a node that already has this Custom Attribute: `com.hp.nnm.topo.TZ`, look for the following message in the `nnm.log` file: Node *<Node name, hostname, management address or UUID>*/*<Management.Address>* has invalid TimeZone value: *<value>*. NNMi stores the log files in the following directory (see About Environment Variables for more information): *%g* = represents the archive number of the archived log file • **Windows**: *%NnmDataDir%*\log\nnm\nnm.log.%g • **Linux**: *$NnmDataDir*/log/nnm/nnm.log.%g For more information, see the "NNMi Logging" chapter in the *HPE Network Node Manager i Software Deployment Reference*, which is available at: http://softwaresupport.hpe.com.)

Chapter 7: Exploring SNMP MIB Source Information

The **MIB file**[1] (source text file) is the basic building block of the SNMP communication protocol. Each entry in a MIB file represents a piece of information you can gather from or change on devices in your network upon demand.

NNMi includes many MIB files and your NNMi Administrator can install any number of additional MIB files.

You can explore the information available in each MIB file in several ways:

- NNMi provides a MIB form that makes it easy to explore the information. See "MIB Form" below.
- You can inspect the MIB's source text file. See "Display a MIB File (source text file)" on page 346.
- You can see a list of all available choices (called MIB Variables) in the **Inventory** workspace, **MIB Variables** view. See "MIB Variables View (Inventory)" on page 52.

Note: If your NNMi role allows, you can use the MIB file to interactively gather data from devices in your network and change settings on network devices. See "Using the MIB Browser" on page 348. For example:

`.1.3.6.1` is the base of the Internet MIB structure.

`.1.3.6.1.2.1` is the base of the MIB-2 branch.

`.1.3.6.1.3` is the base of all MIB objects that are for experimental purposes.

`.1.3.6.1.4.1.9` is the base of all MIB objects provided by Cisco.

`.1.3.6.1.4.1.11` is the base of all MIB objects provided by HP.

`.1.3.6.1.5` is the base of the Security MIB branch.

`.1.3.6.1.6` is the base of the SNMPv2c MIB branch.

MIB Form

The MIB form provides details about the selected MIB file that is loaded on the NNMi management server.

For information about each tab:

To view the MIB Form:

Level-2 Operators and above, do one of the following:

- Method one, in any map or Node table view:
  a. Click or right-click a Node:

[1]Management Information Base files are the basic building block of SNMP communication protocol. SNMP Agents are configured to respond to requests defined by a group of supported MIB files.

- Click and select **Actions → MIB Information → List Supported MIBs**.
- Right-click and select **MIB Information → List Supported MIBs**.

b. Click the link to the MIB file of interest.

- Method two, in the **Inventory** workspace, **MIB Variables** view:

a. Double-click a row to open a MIB Variable form.

b. Navigate to the **MIB** attribute, click the drop-down, and select Open.

- Method three, alternate path for NNMi administrators:

a. Open the **Configuration** workspace, **MIBs** folder.

b. Open the **Loaded MIBs** view.

c. Double-click the row of interest.

MIB Basics Attributes

Attribute	Description
Name	Name from the DEFINITIONS clause within the MIB file.
MIB File	Location of the MIB file on the NNMi server.

MIB Form: MIB Variable Tab

The MIB form's MIB Variables tab lists all MIB variables available within the currently displayed MIB file.

Tip: To view a list of all MIB Variables from all MIB files:

- Level-2 Operators and above can use the **Inventory** workspace, **MIB Variables** view.
- NNMi administrators can use the **Configuration** workspace, **MIBs** folder, **MIB Variables** view.

For information about each tab:

MIB Variables Tab

Attribute	Description
OID (Numeric)	The numeric representation of the OID (Object Identification) value for the selected MIB variable. For example, `IF-MIB`'s `ifAdminStatus` variable: `.1.3.6.1.2.1.2.2.1.7`
Name	The Name value that is stored in the MIB definition for the selected MIB variable. For example, `IF-MIB`'s variable: `ifAdminStatus`
Syntax	The SYTNAX value for the MIB variable. Valid values for MIB variable that can be included in a MIB Expression include the following:

MIB Variables Tab, continued

Attribute	Description

Possible Syntax Values (* = SNMP v1 only, ** = SNMP v2 only)

Syntax	Syntax
Address	** Module Identity
** Agent Capabilities	** Notification Group
Bits	** Notification Type
Counter	** Object Group **
Counter32	Object Identifier
Counter64	** Object Identity
* Display String	Octet String
Enumeration	Opaque
Gauge	Other (Usually indicates = unset)
Gauge32	* Physical Address
Integer	Sequence
Interger32	Sequence of
IP Address	** Textual Convention
MIB Defined (Indicates a custom type defined in the MIB)	Time_Ticks
** Module Compliance	Unsigned32 (Integer)

For example, the `IF-MIB`'s `ifAdminStatus` variable's `SYNTAX`:

```
ifAdminStatus OBJECT-TYPE
   SYNTAX  INTEGER {
       up(1),      -- ready to pass packets
       down(2),
       testing(3)  -- in some test mode
}
```

For more information, click here.

- 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:

MIB Variables Tab, continued

Attribute	Description
	`(((ifInOctets+ifOutOctets)*8/ifSpeed)*100)/sysUpTime*0.01` **Tip:** The sysUpTime variable is a value of hundredths of a second. When you want the rate in seconds, use `sysUpTime*0.01` in the MIB expression as shown in the previous example. • 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.
OID (Text)	The textual representation of the OID for the selected MIB variable. For example, the `IF-MIB`'s `ifAdminStatus` variable: `.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifAdminStatus` Double-click the row representing a MIB variable. The "MIB Variable Form" below displays all details about the selected MIB variable.

MIB Variable Form

The MIB Variable form enables you to view more detailed information about the selected MIB variable provided by a MIB file loaded on the NNMi management server.

For example, the `IF-MIB's ifAdminStatus`:

```
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 that no operational packets can be passed."
 ::= { ifEntry 7 }
```

For information about each tab:

To view the MIB Variable form:

1. Level-2 Operators and above, do one of the following:

Method one, from the Inventory workspace:

- Navigate to the **Inventory** workspace, **MIB Variables** view:
- Click the row containing the MIB variable of interest.

Method two, using Actions:

a. In any map or Node table view, do one of the following:
   - Click a Node and select **Actions → MIB Information → List Supported MIBs**.
   - Right-click a Node and select **MIB Information → List Supported MIBs**.

b. Click the link to the MIB file of interest.

c. Navigate to the **MIB Variables** tab.

d. Select the OID (Numeric) of interest to open an MIB Variable form.

Method three, for NNMi administrators using the Configuration workspace:

- To view information about one MIB file, open the **Configuration** workspace, **MIBs** folder, **Loaded MIBs** view.
  i. Double-click the row of interest.
  ii. Navigate to the **MIB Variables** tab.
  iii. Select the OID (Numeric) of interest to open an MIB Variable form.
- To view information from all MIB files combined, open the **Configuration** workspace, **MIBs** folder, **MIB Variables** view.

  Select the OID (Numeric) of interest to open an MIB Variable form.

2. (*Optional*) To gather this information from a node, see "Run SNMP Walk Commands (MIB Browser)" on page 351.

MIB Variable Basic Attributes

Attribute	Description
Name	The Name value that is stored in the MIB definition for the selected MIB variable. For example **`ifAdminStatus`**
OID (Numeric)	The numeric representation of the OID (Object Identification) value for the selected MIB variable. For example: `.1.3.6.1.2.1.2.2.1.7`
OID (Text)	A symbolic OID uses mnemonic keywords to specify the managed object. For example: `.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifAdminStatus`
Syntax	The SYTNAX value for the MIB variable.

MIB Variable Basic Attributes, continued

Attribute	Description

	For example, the `IF-MIB`'s `ifAdminStatus` variable's `SYNTAX`:
	`ifAdminStatus OBJECT-TYPE`
	`SYNTAX INTEGER {`
	`up(1), -- ready to pass packets`
	`down(2),`
	`testing(3) -- in some test mode`
	`}`
	For more information, click here.
	• 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:
	`(((ifInOctets+ifOutOctets)*8/ifSpeed)*100)/sysUpTime*0.01`
	Tip: The sysUpTime variable is a value of hundredths of a second. When you want the rate in seconds, use `sysUpTime*0.01` in the MIB expression as shown in the previous example.
	• 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.

Textual Convention	Defines the format rules to be used when displaying the MIB value. See "Textual Convention Form" on page 342 for more information.
MIB	The name value that is stored at the beginning of the MIB definitions to identify the MIB. For example, `RFC1213-MIB` is the name of the MIB: `RFC1213-MIB DEFINITIONS ::= BEGIN` **Tip:** To explore *all of the information available* from this MIB, click the Lookup icon, and select Open.
Description	The Description that is stored in the MIB for the selected MIB variable. For example, the `ifDescr` variable's (1.3.6.1.2.1.2.2.1.2) definition in `RFC2233 IF-MIB`: `DESCRIPTION`

MIB Variable Basic Attributes, continued

Attribute	Description
	"A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the interface hardware/software."

MIB Variable Form: Enumerated Values Tab

The Enumerated Values tab enables you to view each enumerated value pair, if any, for a selected MIB OID. For example, the `IF-MIB's ifAdminStatus` includes three enumerated values for status 1=up, 2=down, 3=testing, as shown in the following example:

```
ifAdminStatus OBJECT-TYPE
SYNTAX INTEGER {
1 up,
2 down),
3 testing
 }
 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 }
```

For information about each tab:

Enumerated Value Tab

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. Double-click the row representing an enumerated value pair. The "MIB Variable: Enumerated Values Form" below displays all details about the selected enumerated value pair.

MIB Variable: Enumerated Values Form

The Enumerated Values form edisplays the details of an enumerated value pair, if any, for a selected MIB variable. For example, the `IF-MIB's ifAdminStatus`, includes enumerated values for status as shown in the following example:

```
ifAdminStatus OBJECT-TYPE
SYNTAX INTEGER {
1 up,
2 down),
3 testing
```

```
 }
 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 }
```

To view the Enumerated Value form:

1. Level-2 Operators and above, do one of the following:

   Method one, from the Inventory workspace:

   - Navigate to the **Inventory** workspace, **MIB Variables** view:
   - Click the row containing the MIB variable of interest.

   Method two, using Actions:

   a. In any map or Node table view, do one of the following:
      - Click a Node and select **Actions** → **MIB Information** → **List Supported MIBs**.
      - Right-click a Node and select **MIB Information** → **List Supported MIBs**.

   b. Click the link to the MIB file of interest.

   c. Navigate to the **MIB Variables** tab.

   d. Select the OID (Numeric) of interest to open an MIB Variable form.

   Method three, for NNMi administrators using the Configuration workspace:

   - To view information about one MIB file, open the **Configuration** workspace, **MIBs** folder, **Loaded MIBs** view.
     i. Double-click the row of interest.
     ii. Navigate to the **MIB Variables** tab.
     iii. Select the OID (Numeric) of interest to open an MIB Variable form.
   - To view information from all MIB files combined, open the **Configuration** workspace, **MIBs** folder, **MIB Variables** view.

     Select the OID (Numeric) of interest to open an MIB Variable form.

2. Navigate to the **Enumerated Values** tab.

   This table displays the string and numeric value for each enumeration, if any, specified for the selected MIB variable.

3. Select the String Value of interest to open the Enumerated Values form.

Enumerated Value Basic Attributes

Attribute	Description
String Value	The text value that is associated with the Numeric Value for the selected MIB variable.

Enumerated Value Basic Attributes, continued

Attribute	Description
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, `ifAdminStatus` is an `IF-MIB` OID that contains enumerated values.
MIB	The name value that is stored at the beginning of the MIB definitions to identify the MIB. For example, `IF-MIB` is the name of the MIB: `IF-MIB DEFINITIONS ::= BEGIN` **Tip:** To explore *all of the information available* from this MIB, click the Lookup icon, and select Open.

MIB Variable Form: Table Indices Tab

The Table Indices tab enables you to view the index values, if any, for a selected MIB variable. Table indices are used to store multiple values for a single MIB variable.

In the example, `atIfIndex` and `atNetAddress` are table indices for the `RFC1213-MIB's atEntry` variable. Table indices are identified using the INDEX keyword:

```
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 }
```

For information about each tab:

Table Indices Tab

Attribute	Description
Position	The position number of the MIB variable that is used as a Table Index object. For example, Table Index object positions for `atIfIndex` = 0 and `atNetAddress` = 1: `INDEX { atIfIndex,`

Table Indices Tab, continued

Attribute	Description
	`atNetAddress }`
Name	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. Double-click the row representing a Table Index. The "Table Index Form" below displays all details about the selected Table Index.

Table Index Form

The Table Index form defines one of the multiple-choice values allowed within a single MIB variable.

In the example, `atIfIndex` and `atNetAddress` are table indices for the `RFC1213-MIB's atEntry` variable. Table indices are identified using the INDEX keyword:

```
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 }
```

To view the Table Index form:

1. Level-2 Operators and above, do one of the following:

   Method one, from the Inventory workspace:

   - Navigate to the **Inventory** workspace, **MIB Variables** view:
   - Click the row containing the MIB variable of interest.

   Method two, using Actions:

   a. In any map or Node table view, do one of the following:
      - Click a Node and select **Actions** → **MIB Information** → **List Supported MIBs**.
      - Right-click a Node and select **MIB Information** → **List Supported MIBs**.

   b. Click the link to the MIB file of interest.

   c. Navigate to the **MIB Variables** tab.

   d. Select the OID (Numeric) of interest to open an MIB Variable form.

   Method three, for NNMi administrators using the Configuration workspace:

   - To view information about one MIB file, open the **Configuration** workspace, **MIBs** folder, **Loaded MIBs** view.

i. Double-click the row of interest.
ii. Navigate to the **MIB Variables** tab.
iii. Select the OID (Numeric) of interest to open an MIB Variable form.

- To view information from all MIB files combined, open the **Configuration** workspace, **MIBs** folder, **MIB Variables** view.

  Select the OID (Numeric) of interest to open an MIB Variable form.

2. Navigate to the **Table Indices** tab.

   This table displays the position and name value for each index entry, if any, specified for the selected MIB Variable.
3. Select the Position of interest to open the Table Index form.

Table Index Basic Attributes

Attribute	Description
Position	The position number of the MIB variable that is used as a Table Index object. For example, Table Index object positions `atIfIndex` = 0 and `atNetAddress` = 1: `INDEX { atIfIndex, atNetAddress }`
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 definition text provided in the MIB. For example, `atEntry` is the MIB variable that defines the MIB table: `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 }`
MIB Name	The name value that is stored at the beginning of the MIB definitions to identify the MIB. For example, `RFC1213-MIB` is the name of the MIB: `RFC1213-MIB DEFINITIONS ::= BEGIN` **Tip:** To explore *all of the information available* from this MIB, click the Lookup icon, and select Open.

MIB Form: MIB Notifications Tab

The MIB form's MIB Notifications tab lists each SNMP trap enabled by the currently displayed MIB file.

Tip: To view a list of all MIB Notifications from all MIB files, NNMi administrators can use the **Configuration** workspace, **MIBs** folder, **MIB Notifications** view.

For information about each tab:

MIB Notifications Tab

Attribute	Description
OID (Numeric)	The numeric representation of the OID (Object Identification) value for the selected MIB notification. For example: `.1.3.6.1.6.3.1.1.5.3`
Name	The Name value that is stored in the MIB definition for the selected MIB notification. For example: `linkDown`
OID (Text)	The textual representation of the OID for the selected MIB variable. For example: `.iso.org.dod.internet.snmpV2.snmpModules.snmpMIB .snmpMIBObjects.snmpTraps.linkDown` Double-click the row representing a notification. The "MIB Notification Form" below displays all details about the selected notification.

MIB Notification Form

The MIB Notification form enables you to view the SNMP trap information, if any, that is defined by the selected MIB. For example, the `IF-MIB's linkDown`, includes notification values as shown in the following example:

```
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 }
```

For information about each tab

To view the MIB Notification form:

1. Level-2 Operators and above, do one of the following:

   Method one, using Actions:

   a. In any map or Node table view, do one of the following:
      - Click a Node and select **Actions** → **MIB Information** → **List Supported MIBs**.
      - Right-click a Node and select **MIB Information** → **List Supported MIBs**.
   b. Click the link to the MIB file of interest.
   c. Navigate to the **MIB Notifications** tab.
   d. Select the OID (Numeric) of interest to open an MIB Notifications form.

   Navigate to the **MIB Variables** tab.

   Method two, for NNMi administrators using the Configuration workspace:

   a. Open the **Configuration** workspace, **MIBs** folder.
   b. Open the **Loaded MIBs** view.
   c. Double-click the row of interest.
   d. Navigate to the **MIB Notifications** tab.
   e. Select the OID (Numeric) of interest to open an MIB Notifications form.

2. (*Optional*) To gather this information from a node, see "Run SNMP Walk Commands (MIB Browser)" on page 351.

MIB Notification Basic Attributes

Attribute	Description
Name	The Name value that is stored in the MIB definition for the selected MIB notification. In the following example, `linkDown` is the Name of the MIB variable : **`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 }`
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	The name value that is stored at the beginning of the MIB definitions to identify the MIB. For example, `IF-MIB` is the name of the MIB:

MIB Notification Basic Attributes, continued

Attribute	Description
	`IF-MIB DEFINITIONS ::= BEGIN` **Tip:** To explore *all of the information available* from this MIB, click the Lookup icon, and select Open.
Description	SNMP Trap Description that is stored in the MIB.
Type	*Optional*. SNMP Trap --#TYPE value that is stored in the MIB.
Summary	*Optional*. The --#SUMMARY value that is stored in the MIB for the SNMP Trap.
Arguments	*Optional*. Number of arguments for the SNMP Trap.
Severity	*Optional*. The --#SEVERITY value that is stored in the MIB for the SNMP Trap.
Generic	*Optional*. The --#GENERIC value that is stored in the MIB for the SNMP Trap.
Category	*Optional*. The --#CATEGORY value that is stored in the MIB for the SNMP Trap.
Source ID	*Optional*. The --#SOURCE ID value that is stored in the MIB for the SNMP Trap.
State	*Optional*. The --#STATE value that is stored in the MIB for the SNMP Trap.

MIB Notification Form: Notification Variables Tab

The MIB Notification form's Notification Variables tab enables you to view the SNMP trap information, if any, that can be sent by the selected MIB. In the following example, the `IF-MIB's linkDown` OID provides an SNMP trap. When this trap is generated, the `ifIindex`, `ifAdminStatus`, and `ifOperStatus` values are included in the SNMP trap text:

```
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 }
```

For information about each tab:

MIB Notification Tab

Attribute	Description

Position	The position number of the MIB variable in the Notification Variable object's definition.
	In the following example, `atIfIndex` is position 1, `ifAdminStatus` is position 2, and `ifOperStatus` is position 3:
	`linkDown NOTIFICATION-TYPE`
	`OBJECTS {ifIndex, ifAdminStatus, ifOperStatus}`

Name	The name of the MIB variable.
	In the following example `ifIndex`, `ifAdminStatus`, and `ifOperStatus` are Notification Variables:
	`linkDown NOTIFICATION-TYPE`
	`OBJECTS { ifIndex, ifAdminStatus, ifOperStatus }`
	Double-click the row representing a Table Index. The "Notification Variable Form" below displays all details about the selected Table Index.

Notification Variable Form

The Notification Variables form displays the information that will be included when the SNMP trap is generated. In the following example, the `IF-MIB's linkDown` OID provides an SNMP trap. When this trap is generated, the `ifIindex`, `ifAdminStatus`, and `ifOperStatus` values are included in the SNMP trap text:

```
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 }
```

To view the Notification Variable form:

1. Level-2 Operators and above, do one of the following:
   - Method one, in any map or Node table view:
     i. Click or right-click a Node:
        - Click and select **Actions → MIB Information → List Supported MIBs**.
        - Right-click and select **MIB Information → List Supported MIBs**.
     ii. Click the link to the MIB file of interest.
   - Method two, in the **Inventory** workspace, **MIB Variables** view:

i. Double-click a row to open a MIB Variable form.

ii. Navigate to the **MIB** attribute, click the drop-down, and select Open.

- Method three, alternate path for NNMi administrators:

i. Open the **Configuration** workspace, **MIBs** folder.

ii. Open the **Loaded MIBs** view.

iii. Double-click the row of interest.

2. Navigate to the **MIB Notifications** tab.
3. Select the OID (Numeric) of interest to open an MIB Notification form.
4. Navigate to the **Notification Variables** tab.

   This table displays the string and numeric value for each notification, if any, specified for the selected MIB Notification.
5. Select the Position of interest to open the Notification Variable form.

MIB Notification Basic Attributes

Attribute	Description

Position	The position number of the MIB variable that is used as a Notification Variable object.
	In the following example, `atIfIndex` is position 1, `ifAdminStatus` is position 2, and `ifOperStatus` is position 3:
	`linkDown NOTIFICATION-TYPE`
	`OBJECTS {ifIndex, ifAdminStatus, ifOperStatus}`

MIB Variable	The name of the MIB variable.
	In the following example `ifIndex`, `ifAdminStatus`, and `ifOperStatus` are Notification Variables:
	`linkDown NOTIFICATION-TYPE`
	`OBJECTS { ifIndex, ifAdminStatus, ifOperStatus }`

Trap Definition	The name of the MIB notification used to define the SNMP trap. For example: `linkDown`.
MIB	The name value that is stored at the beginning of the MIB definitions to identify the MIB. For example, `IF-MIB` is the name of the MIB: `IF-MIB DEFINITIONS ::= BEGIN` **Tip:** To explore *all of the information available* from this MIB, click the Lookup icon, and select Open.

MIB Form: Textual Conventions Tab

The MIB form's MIB Textual Conventions tab lists all the format rules defined in the currently displayed MIB file. NNMi uses these MIB format rules to determine how to display any associated MIB variable values.

Tip: To view a list of all Textual Conventions from all MIB files, NNMi administrators can use the **Configuration** workspace, **MIBs** folder, **Textual Conventions** view.

For information about each tab:

Textual Conventions Tab

Attribute	Description
Name	The Name value that is stored in the MIB definition for the selected textual convention. For example: `MAC Address`
Display Hint	Format rule used with the Value Constraint and Primitive Type to help determine the format when displaying the associated MIB value. For example: for `MAC Address`, the Display Hint is `"1x:"` to indicate the value must consist of a one-byte hex string or two-hex digits, such as `01` or `AB`.
Primitive Type	Defines the base type to be used when determining the format for displaying the associated MIB variable value. For example: for the `MAC Address` variable, the Primitive Type is `OCTET STRING`.
Value Constraint	Format rule used with the Display Hint and Primitive Type to help determine the format when displaying the associated MIB variable value. For example: for the `MAC Address` value contraint is `(SIZE (6))` to indicate the format must include six one-byte hex strings, such as `0A:BC:1D:2E:3F:40`. Double-click the row representing an enumerated value pair. The "Textual Convention Form" below displays all details about the selected enumerated value pair.

Textual Convention Form

The MIB Textual Convention form displays format rules for the selected Textual Convention value. MIB files define any required Textual Conventions for their MIB Variables and MIB Notifications. NNMi uses these MIB format rules for determining how to display any associated MIB values.

For information about each tab:

To view the MIB's Textual Convention form:

Level-2 Operators and above, do one of the following:

Method one, using Actions:

1. In any map or Node table view, do one of the following:
   - Click a Node and select **Actions** → **MIB Information** → **List Supported MIBs**.
   - Right-click a Node and select **MIB Information** → **List Supported MIBs**.
2. Click the link to the MIB file of interest.
3. Navigate to the **Textual Conventions** tab.
4. Select the Name of interest to open an MIB Textual Convention form.

Method two, for NNMi administrators:

- To view information about one MIB file, open the **Configuration** workspace, **MIBs** folder, **Loaded MIBs** view.
  a. Double-click the row of interest.
  b. Navigate to the **Textual Conventions** tab.
  c. Select the Name of interest to open an MIB Textual Convention form.
- To view information from all MIB files combined, open the **Configuration** workspace, **MIBs** folder, **Textual Conventions** view.

  Select the Name of interest to open a MIB Textual Convention form.

Textual Conventions Basic Attributes

Attribute	Description
Name	The Name value that is stored in the MIB file's definition for the selected textual convention.
Status	The Status value that is stored in the MIB file's definition for the selected textual convention. Possible values are: • current • deprecated • obsolete
Display Hint	Format rule used with the Value Constraint and Primitive Type to help determine the format when displaying the associated MIB value. For example, to display the MAC Address, the DISPLAY-HINT is `"1x:"` to indicate the value must consist of a one-byte hex string or two-hex digits, such as `01` or `AB`.
Value Constraint	Format rule used with the Display Hint and Primitive Type to help determine the format when displaying the associated MIB variable value. For example, the value constraint under SYNTAX for the MAC Address is `(SIZE (6))` to indicate the format must include six one-byte hex strings, such as `0A:BC:1D:2E:3F:40`.
Primitive Type	Defines the base type to be used when determining the format for displaying the associated MIB variable value. For example, `Octet String` or `Gauge`.
MIB	The name value that is stored at the beginning of the MIB File to identify the MIB. See

Textual Conventions Basic Attributes, continued

Attribute	Description
	"Display a MIB File (source text file)" on page 346. **Tip:** To explore *all of the information available* from this MIB, click the Lookup icon, and select Open to open the "MIB Form" on page 326.
Description	The Description that is stored in the MIB for the selected Textual Convention.

Textual Convention Form: Enumerated Values Tab

The Enumerated Values tab enables you to view each enumerated value pair, if any, for a selected MIB OID. For example, the `IF-MIB's ifAdminStatus` includes three enumerated values for status 1=up, 2=down, 3=testing, as shown in the following example:

```
ifAdminStatus OBJECT-TYPE
SYNTAX INTEGER {
1 up,
2 down),
3 testing
 }
 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 }
```

For information about each tab:

Enumerated Value Tab

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. Double-click the row representing an enumerated value pair. The "Textual Convention: Enumerated Values Form" below displays all details about the selected enumerated value pair.

Textual Convention: Enumerated Values Form

The Enumerated Values form displays the details of an enumerated value pair, if any, for a selected MIB variable. For example, the `IF-MIB's ifAdminStatus` variable includes enumerated values for three statuses, as shown in the following example from the MIB file's source text file:

```
ifAdminStatus OBJECT-TYPE
SYNTAX INTEGER {
1 up,
2 down),
3 testing
 }
 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 }
```

To view the Enumerated Value form:

1. Level-2 Operators and above, do one of the following:

   Method one, using Actions:

   a. In any map or Node table view, do one of the following:
      - Click a Node and select **Actions** → **MIB Information** → **List Supported MIBs**.
      - Right-click a Node and select **MIB Information** → **List Supported MIBs**.

   b. Click the link to the MIB file of interest.

   c. Navigate to the **Textual Conventions** tab.

   d. Select the Name of interest to open an MIB Textual Convention form.

   Method two, for NNMi administrators:

   - To view information about one MIB file, open the **Configuration** workspace, **MIBs** folder, **Loaded MIBs** view.
     i. Double-click the row of interest.
     ii. Navigate to the **Textual Conventions** tab.
     iii. Select the Name of interest to open an MIB Textual Convention form.

   - To view information from all MIB files combined, open the **Configuration** workspace, **MIBs** folder, **Textual Conventions** view.

     Select the Name of interest to open a MIB Textual Convention form.

2. Navigate to the **Enumerated Values** tab.

   This table displays the string and numeric value for each enumeration, if any, specified for the selected MIB variable.

3. Select the String Value of interest to open the Enumerated Values form.

Enumerated Value Basic Attributes

Attribute	Description
String Value	The text value that is associated with the Numeric Value for the selected MIB variable.
Numeric	The numeric value that is associated with the String Value for the selected MIB variable.

Enumerated Value Basic Attributes, continued

Attribute	Description
Value	
MIB Variable	The name of the selected MIB variable that contains enumerated values. For example, `ifAdminStatus` is an `IF-MIB` OID that contains enumerated values.
MIB	The name value that is stored at the beginning of the MIB definitions to identify the MIB. For example, `IF-MIB` is the name of the MIB: `IF-MIB DEFINITIONS ::= BEGIN` **Tip:** To explore *all of the information available* from this MIB, click the Lookup icon, and select Open.

Display a MIB File (source text file)

Inspecting a **MIB file**[1] is useful for determining the date the MIB file was last updated, as well as seeing the syntax for writing MIB files.

There are multiple access points for displaying the MIB file source.

From the MIB Variables View:

1. NNMi Level-2 Operators and above:
   Navigate to the **Inventory** → **MIB Variables** view.
2. Select any row representing a MIB variable.
3. Do one of the following:
   - Click **Actions** → **Display MIB File**.
   - Right-click the row and select **Display MIB File**.
4. NNMi displays the MIB file's source text file.

From the MIB Form:

1. Open the MIB of interest using the "MIB Form" on page 326.
2. Click **Actions** → **Display MIB File**.
3. NNMi displays the MIB file's source text file.

From the MIB Browser:

[1]Management Information Base files are the basic building block of SNMP communication protocol. SNMP Agents are configured to respond to requests defined by a group of supported MIB files.

1. "Using the MIB Browser" on page 348, open the MIB of interest.
2. Generate SNMP Walk results for the MIB of interest.
3. Select a row in the results, and click **Tools** → **Display MIB File**.
4. NNMi displays the MIB file's source text file.

Determine which MIBs a Specific Node Supports

When troubleshooting a problem, it is helpful to know which MIB files are supported by the troubled Node's SNMP Agent. Then you can determine which MIB Variables are available to help you resolve the problem.

To explore the MIBs supported on a selected Node:

1. Do one of the following:
   - Select the Node in any map or table view.
   - Select an Incident in an Incident view, and navigate to the Incident's Source Node form.
2. Select **Actions** → **MIB Information** → **List Supported MIBs**.

   Tip: You can also right-click any object in a table or map view to access the items available within the **Actions** menu.
3. If SNMP communications between NNMi and the Node are working, you will see the list of MIB files currently supported by the Node's associated SNMP Agent.

   Note: If the menu item List Supported MIBs is greyed-out, NNMi does not have access to SNMP communications with this Node. Contact your NNMi administrator to request Communication Configuration settings that establish SNMP communications with this Node.
4. To learn which information can be provided by each MIB file, do the following:
   - Click the displayed link to open a "MIB Form" on page 326. and explore the contents of that MIB file.
   - Within the MIB form, click **Actions** → **Display MIB File** to read the actual source text of the MIB file, if you prefer that format. See "Display a MIB File (source text file)" on the previous page.
5. See "Using the MIB Browser" on page 348 to gather the current MIB Variable values being reported by the SNMP Agent assigned to a Node.

Chapter 8: Using the MIB Browser

When investigating and diagnosing network problems, it may be useful to query a node for SNMP MIB Variable values. This technique can provide real-time information about the node that is *in addition* to that information stored in the NNMi database.

Note: Access to these commands depends on the **NNMi Role**[1] and Object Access Privileges to which you are assigned. If you are unable to access an action, contact your NNMi administrator.

If your NNMi Security Settings allow, you can use NNMi's MIB Browser to perform the following tasks:

- **SNMP Walk**
  This command gathers real-time responses to one or more questions (MIB Variables). The range and complexity of the queries is limited only by the target Node's associated SNMP Agent configuration for **MIB file**[2] support.

  In the MIB Browser, specify Node and the query starting point (OID of the MIB), then click the **Walk** button to generate responses from the SNMP Agent for MIB Variables from any designated starting point down though the MIB structure.

  To display the responses obtained from another location in the Internet MIB structure, change the OID attribute value (MIB object identifier).
- **SNMP Set**
  This command makes a real-time change on the target Node. For example, you could issue an SNMP Set for the `SNMPv2-MIB`'s MIB Variable named `sysContact` to let everyone on your team know that you are assigning someone new to that Node.

See the following topics for details:

- MIB Browser Prerequisites 350

[1]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.
[2]Management Information Base files are the basic building block of SNMP communication protocol. SNMP Agents are configured to respond to requests defined by a group of supported MIB files.

- Run SNMP Walk Commands (MIB Browser) 351
- Run SNMP Set Commands (MIB Browser) 356
- Use Aliases in MIB Browser Commands 360
- View MIB Browser Results 361
- Save MIB Browser Results to a CSV File 363
- Print MIB Browser Results 364

MIB Browser Prerequisites

Confirm the following items to ensure best results from your MIB Browser queries:

1. Verify that the Node you want the MIB Browser to query responds to SNMP Get and Set commands. See SNMP Agent State settings on the "Node Form" on page 65.
2. Verify that the MIB files defining the MIB Variables you want to use are supported by the target Node's SNMP Agent. See "Determine which MIBs a Specific Node Supports" on page 347.
3. Verify that the MIB files defining the MIB Variables you want to use are installed on the NNMi management server. See "MIB Variables View (Inventory)" on page 52.
4. Contact your NNMi administrator with requests for loading additional MIB files on Nodes or the NNMi management server.

MIB Browser Menu Items

Menu Item		
Tools	→ **Diplay MIB File**	Displays the MIB File (text source file) where the selected OID is defined. See "Display a MIB File (source text file) " on page 346.
	→ **List Supported MIBs**	Determine which MIBs are installed on the selected Node. The resulting list determines which SNMP Walk and Set choices you have for this Node. Click the links on the displayed list to open a "MIB Form" on page 326. It is easier to review each available MIB Variable within this context than within the source text file.

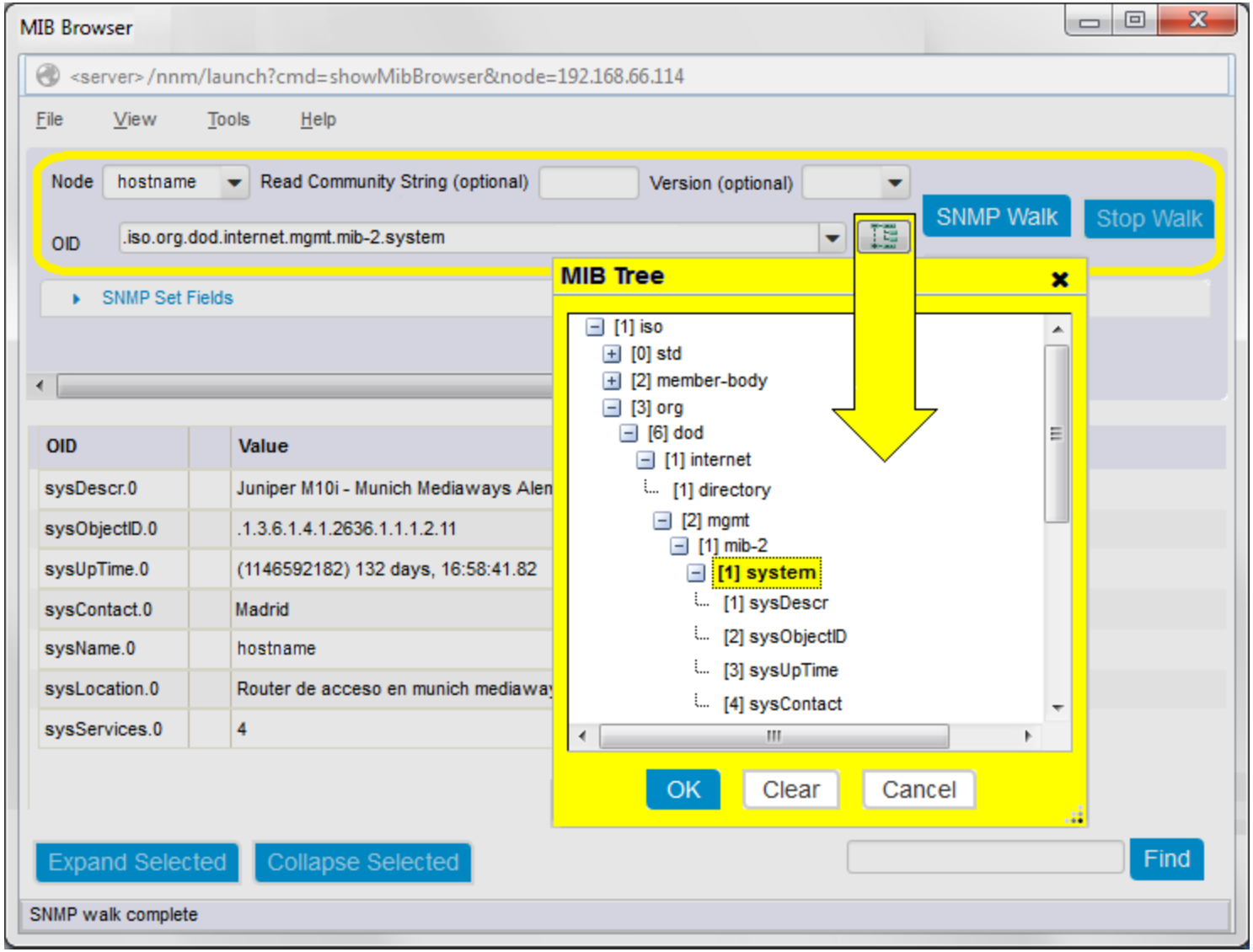
For additional MIB Browser information:

Run SNMP Walk Commands (MIB Browser)

Note: Access to these commands depends on the **NNMi Role**[1] and Object Access Privileges to which you are assigned. If you are unable to access an action, contact your NNMi administrator.

You can use the NNMi MIB Browser to gather a wealth of real-time information from devices in your network environment. The list of available questions are defined in MIB files as MIB Variables, each with a unique OID. See "Exploring SNMP MIB Source Information" on page 326.

[1]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 gather information from a particular Node in your network environment:

1. Verify the "MIB Browser Prerequisites" on page 350.
2. Access the MIB Browser.

   Level-2 Operators and above, do one of the following:

   - Select **Tools** → **MIB Browser**.
   - In any map or Node table view, do one of the following:
     - Click a Node and select **Actions** → **MIB Information** → **MIB Browser**.
     - Right-click a Node and select **MIB Information** → **MIB Browser**
   - In any Incident view, double-click an Incident to open the Incident form:
     i. In the Source Node attribute, click the drop-down, and select Open.
     ii. In the Node form, select **Actions** → **MIB Information** → **MIB Browser**.
   - Within the MIB Form or MIB Variable Form:

     Select **Actions** → **MIB Information** → **MIB Browser**.

3. **Node**: The Node Name or IP address of the Node whose MIB Variable values you want to collect.
4. **Read Community String**: (*Optional*) Do one of the following:
   - Leave this attribute value blank. NNMi uses the *read community string* currently configured for the target Node in NNMi's Communication Configuration settings (without your needing to provide any in the MIB Browser).
   - Enter a valid *read community string* for the Node.
5. **Version (optional)**: Do one of the following:
   - Leave this attribute value blank. NNMi uses the *SNMP version* currently configured for the target Node in NNMi's Communication Configuration settings (without your needing to provide any in the MIB Browser).
   - Select an SNMP version from the drop-down list.

   For a discovered Node: NNMi uses the read community string, SNMP version, timeout, maximum retries, and management address

port currently configured for the target Node in NNMi's Communication Configuration settings for that Node (without your needing to provide any of those values in the MIB Browser).

For an undiscovered Node: NNMi uses default timeout, maximum retries, and management address port parameters provided by the NNMi administrator within the `nms-ui.properties` file. And you must type a value in the MIB Browser's Read Community String field. For more information, see the "Maintaining NNMi" chapter in the *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.

6. **OID**: The MIB's object identifier (number or mnemonic keywords) you want to use for gathering one value or multiple values with the SNMP `Walk`:

   If you access MIB Browser using **Tools** → **MIB Browser** = *the default value is* `.iso.org.dod.internet.mgmt.mib-2.system`

   If you access MIB Browser using **MIB Information** → **MIB Browser** = NNMi populates this attribute with the currently selected view's row or form's MIB Variable value.

   - Numbers must begin with a dot (.)
   - As you type, a list appears assisting with auto-complete possibilities (OID text, numeric, or alias).
   - Click the MIB Tree icon to select the OID of interest. Click one of the following:

     OK = Populates the OID field with the selected value.

     Clear = Deletes any text from the OID field.

     Cancel = Closes the MIB Tree popup.

     Note: The items in the MIB Tree represent all MIB files currently placed in the required location on the NNMi management server's hard drive and Loaded for use. Each MIB Variable may or may not be available *on the Node you querie*.

   - In the results pane, select a row, then **Right-Click** → **Populate Current OID**.

- Click **Tools** → **OID Aliases** to use a shortcut defined by an installed **MIB file**[1] (source text files). See also Use Aliases in MIB Browser Commands.

Tip: The Node's SNMP Agent .responds to `.1.3` with a list of real-time values for *all* currently supported MIB variables. See also "MIB Variables View (Inventory)" on page 52 for more ideas.

7. To see the Node's response to the MIB Browser's request:
   - Press **Enter** or click the **SNMP Walk** button to get SNMP Walk results from your starting point down though the MIB Variables tree.
   - Click the **Stop Walk** button to suspend the operation. (If the text on this button is gray, all data has been collected.)

Tip: If you are gathering SNMP data from a Node that is not currently in the NNMi database, notify your NNMi administrator that SNMP communications with this Node is possible, but not currently configured in NNMi. Request that your NNMi administrator establish Communication Configuration settings for automatic SNMP communication with this Node.

8. Explore the results list. See "View MIB Browser Results" on page 361.

For additional MIB Browser information:

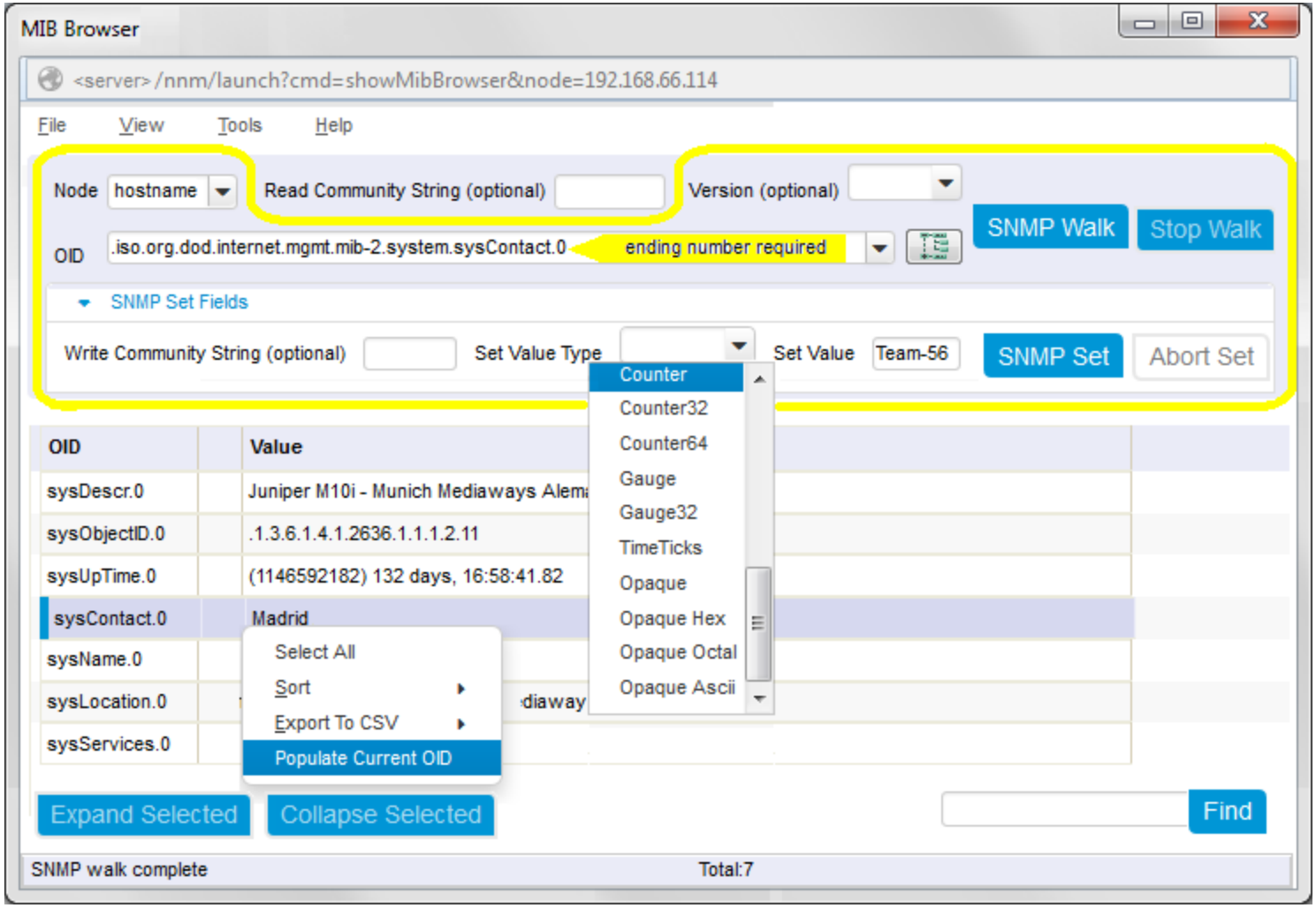
[1]Management Information Base files are the basic building block of SNMP communication protocol. SNMP Agents are configured to respond to requests defined by a group of supported MIB files.

Run SNMP Set Commands (MIB Browser)

Note: Access to these commands depends on the **NNMi Role**[1] and Object Access Privileges to which you are assigned. If you are unable to access an action, contact your NNMi administrator.

You can use the NNMi MIB Browser to change settings on devices in your network environment. The list of available settings are defined in MIB files as MIB Variables, each with a unique OID. See "Exploring SNMP MIB Source Information" on page 326.

[1]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 change information on Nodes in your network environment:

1. Verify the "MIB Browser Prerequisites" on page 350.
2. Access the MIB Browser.

Level-2 Operators and above, do one of the following:

- Select **Tools** → **MIB Browser**.
- In any map or Node table view, do one of the following:
  - Click a Node and select **Actions** → **MIB Information** → **MIB Browser**.
  - Right-click a Node and select **MIB Information** → **MIB Browser**
- In any Incident view, double-click an Incident to open the Incident form:
  i. In the Source Node attribute, click the drop-down, and select Open.
  ii. In the Node form, select **Actions** → **MIB Information** → **MIB Browser**.
- Within the MIB Form or MIB Variable Form:
  Select **Actions** → **MIB Information** → **MIB Browser**.

3. **Node**: The Node Name or IP address of the Node whose MIB Variable values you want to modify.
4. **OID**: The MIB's object identifier (number or mnemonic keywords) you want to use for the SNMP `Set`. Do one of the following:
   - Type the OID you want to use into the OID field.
   - In any displayed previous SNMP Walk results:
     - Right-click any previous SNMP Walk result's end-point (text in the OID column with a number appended to the end), and select **Populate Current OID**.
     - Click the MIB Tree icon to select the OID of interest. Click one of the following:
       OK = Populates the OID field with the selected value.
       Clear = Deletes any text from the OID field.
       Cancel = Closes the MIB Tree popup.
5. **Version (optional)**: Do one of the following:
   - Leave this attribute value blank. NNMi uses the *SNMP version* currently configured for the target Node in NNMi's Communication Configuration settings (without your needing to provide any in the MIB Browser).
   - Select an SNMP version from the drop-down list.

For a discovered Node: NNMi uses the read community string, SNMP version, timeout, maximum retries, and management address port currently configured for the target Node in NNMi's Communication Configuration settings for that Node (without your needing to provide any of those values in the MIB Browser).

For an undiscovered Node: NNMi uses default timeout, maximum retries, and management address port parameters provided by the NNMi administrator within the `nms-ui.properties` file. And you must type a value in the MIB Browser's Read Community String field. For more information, see the "Maintaining NNMi" chapter in the *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.

6. **Write Community String**: (*Optional*) Do one of the following:
   - Leave this attribute value blank. NNMi uses the *write community string* currently configured for the target Node in NNMi's Communication Configuration settings (without your needing to provide any in the MIB Browser).
   - Enter a valid *write community string* for the Node.
7. **Set Value Type**: Click the drop-down list and make your selection.
8. **Set Value**: Provide a numeric or text string appropriate for the value you are changing on the target Node.
9. Click the **SNMP Set** button. NNMi updates the results pane of the MIB Browser to show the Node's response to the SNMP Set request.

Tip: If the MIB Browser hangs due to the Node's SNMP Agent not responding, click the **Abort Set** button to bring NNMi back online.

If the text on the Abort Set button is gray, the target Node's SNMP Agent successfully completed the requested change.

10. Explore the results list. See "View MIB Browser Results" on page 361.

For additional MIB Browser information:

Use Aliases in MIB Browser Commands

The MIB Browser uses the MIB Variable you enter into the **OID** attribute to determine which information is gathered or changed on the target Node. Type that OID value in one of the three formats specified in the MIB File's definition of that MIB Variable:

- The numeric identifier
- The text string identifier
- The alias (short text string)

To understand which particular alias values could save you time, do the following:

1. Navigate to the "MIB Variables View (Inventory)" on page 52.
2. Right-click the **Syntax** column heading and select **Filter** → **Create Filter**.
3. Configure the filter with **Equals** = **Other**. Click **Apply**. The rows now visible in your MIB Variables view are the alias values provided by the MIB Files that are currently loaded onto the NNMi management server.
4. To reduce the list to only those aliases for a particular MIB or MIBs of interest, create a filter for the **MIB** column.
5. Double-click each row to study the definition and understand what the alias can do for you.
6. Now you can access the MIB Browser and copy/paste or type those aliases into the **OID** attribute to configure your query when you do the following:
   - "Run SNMP Walk Commands (MIB Browser)" on page 351
   - "Run SNMP Set Commands (MIB Browser)" on page 356

   Tip: In the MIB Browser, the **Tools** → **OID Aliases** menu item displays a quick-reference list of all available MIB aliases currently loaded on the NNMi management server.

For additional MIB Browser information:

View MIB Browser Results

Prerequisite: Do one of the following:

- "Run SNMP Walk Commands (MIB Browser)" on page 351
- "Run SNMP Set Commands (MIB Browser)" on page 356

To explore the results list:

- Click the Expand icon preceding an entry to expand *one level* deeper.
- Select a row and click **Expand Selected** to expand *all levels* deeper.
- Click the Collapse icon preceding an entry to collapse deeper levels.
- Select a row and click **Collapse Selected** to collapse deeper levels.
- Click a button to display a table of possible choices associated with a multiple-choice OID value.
- Select any row and click **View** → **Quick View** (or double-click) to popup the basic definition of the item.
- Use **Find** at the bottom of the Results pane. Type *the first few letters of an item in Column 1* and click **Find**. Then click the Find button again to move to the next instance of matching initial text in Column 1
  - OID column only
  - Initial text only
  - Case-sensitive

MIB Browser Menu Items

Menu Item	
View	→ **Quick View**
	→ **MIB Table** (alternate access to button results)

MIB Browser Menu Items, continued

Menu Item	
Right-click	→ **Select All**
	→ **Sort** → **Ascending**
	→ **Sort** → **Descending**

The following table describes the keystrokes you can use to navigate the NNMi MIB Browser.

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 Expand icon preceding an entry to expand *one level* deeper.
Shift + Left Arrow	Close an open Collapse icon preceding an entry to collapse deeper levels.
Spacebar	Toggle the table column sort order between ascending and descending order.

For additional MIB Browser information:

Save MIB Browser Results to a CSV File

Prerequisite: Do one of the following:

- "Run SNMP Walk Commands (MIB Browser)" on page 351
- "Run SNMP Set Commands (MIB Browser)" on page 356

You can save your MIB Browser results to a comma separated values (CSV) file, and use those results in other programs of your choice (for example, spreadsheet software programs such as Microsoft Excel).

To save the results to a CSV file, decide whether you want to save all the data within the MIB Browser's results pane, or save a subset of that data. The MIB Browser provides the menu choices in the following table.

When saving a subset of information, use mouse click and shift-clicks for highlighting the block of data to be saved.

MIB Browser Menu Items

Menu Item	
File	→ **Export to CSV** → **All Rows** → **Export to CSV** → **Selected Rows**
Right-click	→ **Export to CSV** → **All Rows** → **Export to CSV** → **Selected Rows**
Right-click	→ **Select All**

For additional MIB Browser information:

Print MIB Browser Results

Prerequisite: Do one of the following:

- "Run SNMP Walk Commands (MIB Browser)" on page 351
- "Run SNMP Set Commands (MIB Browser)" on page 356

You can print MIB Browser results using the MIB Browser's **File** → **Print Visible** menu.

To print MIB Browser output for a selected node:

1. Navigate through the information in the results pane, and display the information that you would like to print:
   - Click the Expand icon preceding an entry to expand *one level* deeper.
   - Select a row and click **Expand Selected** to expand *all levels* deeper.
   - Click the Collapse icon preceding an entry to collapse deeper levels.
   - Select a row and click **Collapse Selected** to collapse deeper levels.
   - Click a button to display a table of possible choices associated with a multiple-choice OID value.
2. To print the visible content, select **File** → **Print Visible**.
3. NNMi sends the visible image to the printer that you specify.

Caution: Only the results area visible on your monitor is included. You must scroll down the results pane and print each visible block if you want all of the results. Consider saving large amounts of results data to a CSV file and using some other tool for the printing. See "Save MIB Browser Results to a CSV File" on the previous page.

MIB Browser Menu Items

Menu Item	
File	→ **Print Visible**
View	→ **Quick View**
	→ **MIB Table** (alternate access to button results)
Right-click	→ **Select All**
	→ **Sort** → **Ascending**
	→ **Sort** → **Descending**

For additional MIB Browser information:

Chapter 9: 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:

- Node Group Maps 368
- Display the Layer 2 Neighbor View 378
- Display the Layer 3 Neighbor View 381
- Path Between Two Nodes that Have IPv4 Addresses 382
- MPLS WAN Cloud Map (NNMi Advanced) 389
- Enhanced Path View (NNMi Advanced) 390

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

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.

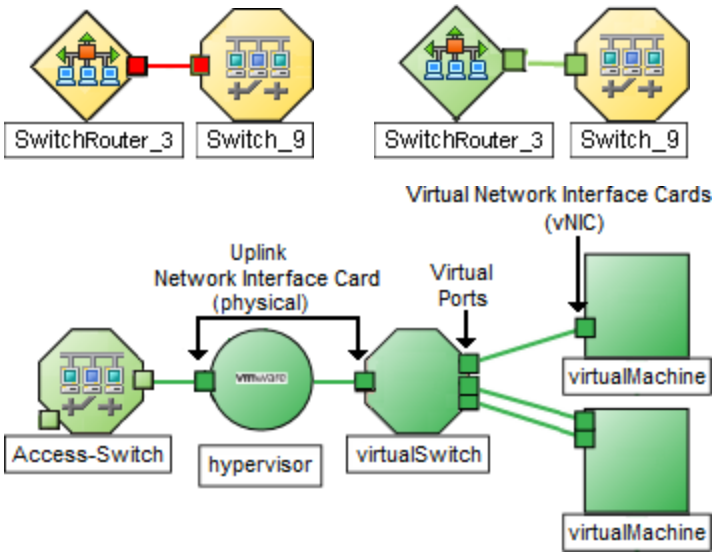
The OSI initiative identified seven layers for communication and computer network protocol design. The **Layer 2**[1] and **Layer 3**[2] Neighbor Views display data according to the Open Systems Interconnection (OSI) model.

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:

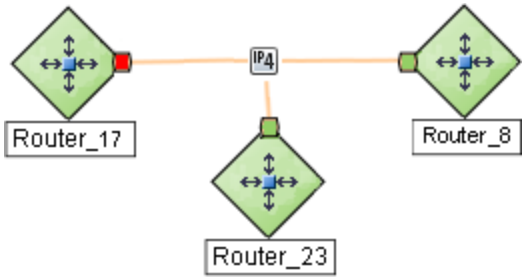
[1]Refers to the Data Link layer of the multilayered communication model, Open Systems Interconnection (OSI). The Data Link layer moves data across the physical links in the network. The switches and switch-routers are devices that redirect data messages at the layer 2 level, using the destination Media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



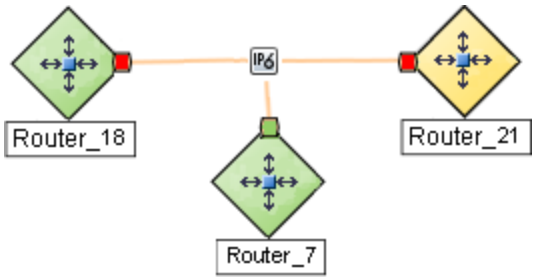
Tip: Right-click any **hypervisor**[1] or one of its resources to see the Wheel Dialog or Loom Dialog.

See About Status Colors for more information.

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



(*NNMi Advanced*) IPv6 subnets are indicated by this symbol:



[1]The virtual machine manager in charge of delegating various aspects from a pool of resources to become virtual devices. The delegations might be static or dynamic, depending on the manufacture's implementation. The type of virtual machines being generated depends on the manufacturer's implementation.

Node Group Maps

The Node Group Maps in the Topology Maps workspace and Troubleshooting workspace 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 also right-click any object in a table or map view to access the items available within 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.
- Select a Node Group map from the **Topology Maps** workspace.
  a. From the **Workspaces** navigation panel, select the **Topology Maps** workspace.
  b. Click to expand **All Node Groups**.
  This folder appears only if you have permission to create and delete Node Groups for the nodes you have permission to access. If you are an Network Node Manager i Software administrator, see the "Maintaining NNMi" chapter in the HPE Network Node Manager i Software Deployment Reference for information about how to enable access to this folder.
  c. Select any Node Group map name that is preceded with the Node Group Map symbol .
  Tip: The following symbol indicates no Node Group Map Settings are configured for the Node Group: .
- 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 299 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**[1]. Use the **Indicate Key Incidents** button in the map view toolbar (see Using the View Toolbars: Node Group Map Toolbar Icons):

  Caution: Pay attention to the highlighting on the button:

  (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**[2]. (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**[3].

  To view the associated incident for the node, double-click the node symbol. In the Node form, select the Incidents tab.

- (*NNM iSPI Performance for Metrics 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 NNM iSPI Performance for Metrics report that are visible in NNMi, use the **Actions → HPE NNM iSPI Performance → Synch Interface and Node 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 374. Your NNMi administrator can provide more Node Group maps.

Related Topics

"Navigating within a Node Group Map" below

"Position Nodes on a Node Group Map" on page 372

"Add Annotations to a Map" on page 372

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:

[1]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.
[2]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.
[3]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: 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 also right-click any object in a table or map view to access the items available within 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**[1]. Use the **Indicate Key Incidents** button in the map view toolbar (see Using the View Toolbars: Node Group Map Toolbar Icons):

  Note: Pay attention to the highlighting on the button:

  (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**[2]. (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**[3].

  To view the associated incident for the node, double-click the node symbol. In the Node form, select the Incidents tab.

[1]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.
[2]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.
[3]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.

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 also right-click any object in a table or map view to access the items available within the **Actions** menu.
2. Manually position node locations within the map to meet your team's needs: Navigate Maps.
3. This placement persists until you refresh or otherwise reload the map.

   Node Group Maps only: If your role permits, click the **Save Map** toolbar button to keep the new layout visible on that map in the future. Once a map is saved, newly discovered devices appear in the bottom left corner of the map.

   Note: Each time you select **Save Map**, NNMi deletes any previous node location information for the map. All team members see the changes.

Related Topics

"Add Annotations to a Map" below

Add Annotations to a Map

Network Node Manager i Software enables you to add annotations to a Node Group map. For example, you might want to label a map with the type of nodes or office location.

Note: You must have permission to create, delete, and modify Node Group maps to use this feature. If you are an NNMi administrator, see the "Maintaining NNMi" chapter in the HPE Network Node Manager i Software Deployment Reference for more information about how to enable this feature.

Use the Map Annotations feature to do any of the following:

Add a map annotation

To add an annotation:

1. Right-click the mouse in an empty space between nodes where you want to add text.
2. Select **Add Map Annotation**.
3. Navigate to the **Annotation Text** attribute and enter the text you want to add to the map.

   Note: Enter a maximum of 2048 characters.

   Adjust the text location within the annotation using the space bar and <Enter>.
4. *Optional*. Select a font from the **Font** menu.
5. *Optional*. Select a text style from the **Style** menu.
6. *Optional*. Select a text size using the Scale menu.

   Annotations retain the scale size selected when you pan and zoom the map
7. *Optional*. Navigate to **Box colors** and select a text color from the **Foreground** menu.
8. *Optional*. Navigate to **Box colors** and select a background color from the **Background** menu.

   Tip: Select **Transparent** if you want anything that appears behind the text annotation (for example, the background image) to show through.
9. *Optional*. Use the **Z-index** option when you have multiple annotations.

   This option enables you to layer annotations by specifying the order placement from front to back of each annotation. The higher the number, the closer the annotation appears in the foreground.

   Select the annotation of interest and enter the **Z-index** value.

   Network Node Manager i Software uses the following display order from front to back:

   - Map
   - Annotations (by Z-index order)
   - Background image
10. Click **Save Map** to save the annotations and node locations.

Move an annotation

To move an annotation:

1. Mouse over the upper left-hand corner of the annotation.

   A black circle appears to indicate the annotation can be moved.
2. Click and drag the text box to the desired location.
3. Click **Save Map** to save the new annotation location.

Modify an annotation

To modify an annotation:

1. Mouse over the upper left-hand corner of the annotation you want to modify.

   A black circle appears to indicate the annotation can be moved or modified.

2. Right-click the black circle and select **Edit**
3. Navigate to each attribute value you want to change.
4. Click **Save Map** to save the annotations and node locations.

Adjust the size of an annotation

To adjust the annotation size:

1. Mouse over the lower left-hand corner of the annotation until a black triangle appears.
2. Drag the triangle to re-size the annotation.

   Note: The selected scale remains the same when you zoom in or out in the map.

3. Click **Save Map** to save the new annotation size.

Copy and paste an annotation to a new location or map.

To copy and paste an annotation:

1. Mouse over the upper left-hand corner of the annotation you want to copy.
2. Right-click in the black circle that appears and select **Copy**.
3. Navigate to the new location.

   Note: You can paste the annotation in any map that is in the NNMi console.

4. Right-click and select **Paste**.

Delete an annotation

To delete an annotation:

1. Mouse over the upper left-hand corner of the annotation you want to remove.

   A black circle appears to indicate the annotation can be moved or modified.
2. Right-click the black circle and select **Delete**.

In Node Group Maps, if your role permits, you can manually reposition symbols on a map and save the location settings. See **Help → Help for Operators** for more information.

Related Topics

Adjust the Zoom Factor

Pan Around the Map

Set the Location of the Overview Pane

Find a Node in a Map

Node Group Overview Map

The **Node Group Overview** map in the Topology Maps workspace displays a map of all top-level Node Groups currently configured for your network.

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

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

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

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

Related Topics

Views of Topology Maps

Node Group Map Objects

Initial Discovery Progress or Network Overview Map

The **Initial Discovery Progress** view in the Topology Maps workspace 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 in the Topology Maps workspace 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 HPE 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 of Topology Maps

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 in the Topology Maps workspace 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:

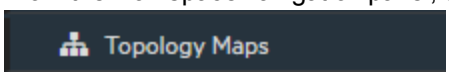
- Chassis
- Firewalls
- Voice Gateways

To view the connectivity within each device type (Node Group), click the Node Group of interest. See "Node Groups View (Inventory)" on page 56 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. Click to expand **Node Group Maps**.
3. Select **Networking Infrastructure Devices**.

Related Topics

Views of Topology Maps

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.

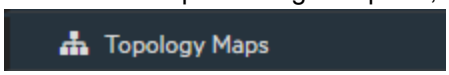
The **Routers** map in the Topology Maps workspace shows a graphical representation of the Layer 3 connectivity in your network. Connector devices on Layer 3 maps are routers, switch-routers, and gateways. (See About Map Symbols for more information.)

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. Click to expand **Quick Access Maps**.
3. Select **Routers**.

Related Topics

Views of Topology Maps

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.

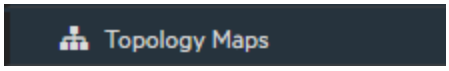
The **Switches** map in the Topology Maps workspace shows a graphical representation of the Layer 2 connectivity in your network. Connector devices on Layer 2 maps are switches, ATM switches, and switch-routers. (See About Map Symbols for more information.)

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. Click to expand **Quick Access Maps**.
3. Select **Switches**.

Related Topics

Views of Topology Maps

Node Group Map Objects

Display the Layer 2 Neighbor View

The **Layer 2**[1] 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).

[1]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.

- 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 65 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.)
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 366).

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

   (older versions of NNMi used)

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 also right-click any object in a table or map view to access the items available within 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 366).

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

   (older versions of NNMi used)

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 255 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 255

Display the Layer 3 Neighbor View

The **Layer 3**[1] 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.
- 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 workpspace:

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 65 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 366).

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** worspace, **Nodes** view.
2. Select the initial object of interest.

[1]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.

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 also right-click any object in a table or map view to access the items available within 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 366).

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 189 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 390.

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 378 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 385). 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" on page 402 for more information about Router Redundancy Groups. See "Path Calculation Rules" on page 385 for more information about Active router paths.
- (*NNMi Advanced*, plus *HPE Route Analytics Management System (RAMS) for MPLS WAN*) HPE 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 390 for more information. If you are an NNMi administrator, see HPE RAMS MPLS WAN Configuration (NNMi Advanced) for information about configuring RAMS.

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.

(*NNM iSPI Performance for Metrics*) You can view a report of the Path Health from the Path View map using the **Actions → HPE 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 -- click here 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 390 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 also right-click any object in a table or map view to access the items available within the **Actions** menu.

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

Related Topics:

"Path Calculation Rules" on the next page

"Investigate Errors and Performance Issues" on page 388

"Access Node Details" on page 409

Path Calculation Rules

Note: If NNMi Advanced is licensed and installed, also see "Enhanced Path View (NNMi Advanced)" on page 390

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

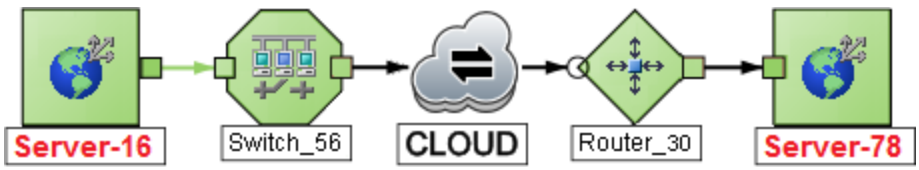
Note: The path calculated can include one or more VLANs when applicable.

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.

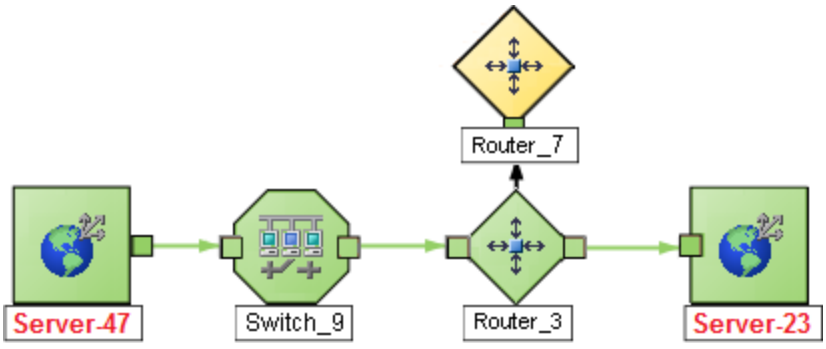
A cloud symbol can represent the following types of information. The map can include multiple cloud symbols:



- 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.

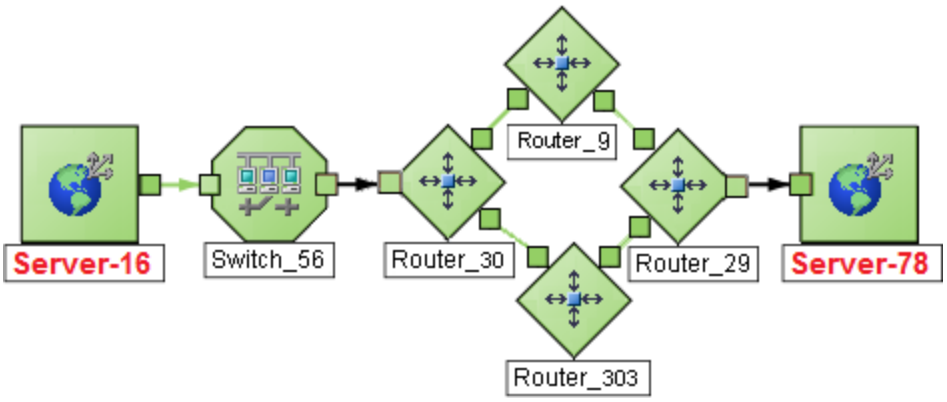
When interpreting Path View results, note the following:

- 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 System (RAMS), the Path View can show multiple **OSPF**[1] Equal Cost paths through a Layer 3 cloud as shown in the example below:

[1]Open Shortest Path First Protocol



If you are an NNMi administrator, see HPE RAMS MPLS WAN Configuration (NNMi Advanced) for information about configuring RAMS.

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 390 for more information.

- (*NNM iSPI Performance for Metrics*) You can access performance data from Path Views that contain single or multiple paths. See "Investigate Errors and Performance Issues" on 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*, plus *HPE Route Analytics Management System (RAMS) for MPLS WAN*) 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 390 for more information. If you are an NNMi administrator, also see HP RAMS MPLS WAN Configuration (NNMi Advanced) 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**[1], 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 406 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 409
- "Access a Problem Device" on page 408
- "Access All Related Incidents" on page 411

  See "Interpret Root Cause Incidents" on page 490 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.

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

To access performance data from a Path View map:

Select **Actions** → **HPE 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** → **HPE NNM iSPI Performance** → **Reporting** - **Path Health**.

[1]Multiprotocol Label Switching

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*)

(*NNMi Advanced*, plus *HPE Route Analytics Management System (RAMS) for MPLS WAN*) 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 WANs in the Network:

Note: After installing and configuring the RAMS Integration Module, NNMi startup discovers all the MPLS WANs 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 WANs in the network.

To display the MPLS WAN Cloud Map view:

1. In the MPLS WAN 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:

MPLS WAN Cloud view symbols

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 Status Color and Meaning for Objects.
	The CE router that is participating in the MPLS WAN cloud.

MPLS WAN Cloud view symbols, continued

Symbol	Description
	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 Status Color and Meaning for Objects.

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 305

"MPLS WAN Cloud (RAMS) Form: MPLS WAN Connections Tab (NNMi Advanced)" on page 306

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**[1] or **VRRP**[2])

  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.
- (*HPE Route Analytics Management System (RAMS) for MPLS WAN*) HPE Router Analytics Management System (**RAMS**[3]) 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.) If you are an NNMi administrator, see HPE RAMS MPLS WAN Configuration (NNMi Advanced) for more information.

  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 HPE Router Analytics Management System (RAMS) determines more than one equal cost path and, therefore, cannot determine which path is in use.

[1]Hot Standby Router Protocol
[2]Virtual Router Redundancy Protocol
[3]HP Router Analytics Management System

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.

Chapter 10: 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 37

"Monitor with Table Views" below

"Monitor with Map Views" on page 405

"Monitor with Graphs" on page 415

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 Sensors View" below

"Non-Normal Physical Sensors View" on the next page

"Non-Normal Chassis View" on page 395

"Non-Normal Cards View" on page 396

"Non-Normal Interfaces View" on page 396

"Non-Normal Nodes View" on page 397

"Non-Normal SNMP Agents View" on page 399

"Not Responding Addresses View" on page 399

"Interface Performance View" on page 400

"Card Redundancy Groups View (Monitoring)" on page 401

"Node Groups View (Monitoring)" on page 403

"Custom Node Collections View" on page 403

"Custom Polled Instances View" on page 404

Non-Normal Node Sensors View

Tip: See "Node Sensor Form" on page 232 for more details about the node sensor attributes that appear in this view's column headings. Node Sensors are displayed in three views: "Node Sensors View" on page 47, "Non-Normal Node Sensors View" above, and "Unmanaged Node Sensors View" on page 585.

The **Non-Normal Node Sensors** view in the Monitoring workspace is useful for identifying all of the Node Sensors that might need operator attention. Examples of Node Sensors include buffers, CPU, disks, and memory.

Possible Statuses for these interfaces include:

Warning

Minor

Major

Critical

To display the Non-Normal Node Sensor view:

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

For each Node Sensor 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 Physical Sensors View

Tip: See "Physical Sensor Form" on page 244 for more details about the node sensor attributes that appear in this view's column headings. Node Sensors are displayed in three views: "Physical Sensors View" on page 47, Non-Normal Physical Sensors View, and "Unmanaged Physical Sensors View" on page 585.

The **Non-Normal Physical Sensors** view in the Monitoring workspace is useful for identifying all of the Physical Sensors that might need operator attention. Examples of Physical Sensors include backplane, fan, power, temperature, and voltage.

Possible Statuses for these interfaces include:

Warning

Minor

Major

Critical

To display the Non-Normal Physical Sensor view:

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

For each Physical Sensor displayed, you can see its Status, Name, Type, the Managed By (Node), Hosted On (chassis in which it resides), and the date and time the Status was last modified.

Related Topics

Use Table Views

Export Table Information

Non-Normal Chassis View

Tip: See "Chassis Form" on page 193 for more details about the chassis attributes that appear in this view's column headings.

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

Warning

Minor

Major

Critical

Note: Chassis displayed in this table all have the AdministrativeState equal to **Up** and a Status *other than* **Normal**.

To display the Non-Normal Chassis view:

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

The columns in this table view show many attributes of each chassis.

By default, this view is sorted by the date the chassis status was last modified.

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

Use	Description
View all network chassis per node	Sort the view using the **Managed By** column. This can help you organize your chassis per node, so that you can identify the nodes that might need attention.
Determine the health of each of the managed chassis	Sort the view by the **Status** attribute.
Determine the types of chassis that are being managed.	Sort on the **ifType** (chassis type) attribute.
Access a map view of the network chassis and its surrounding topology.	Select the chassis of interest and use the **Actions** menu to select either the Layer 2 or Layer 3 Neighbor View. See Use Table Views for more information. **Tip:** You can also right-click any object in a table or map view to access the items available within the **Actions** menu.

Related Topics

Use Table Views

Export Table Information

Non-Normal Cards View

Tip: See "Card Form" on page 211 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. Possible statuses for these cards include:

- Warning
- Minor
- Major
- Critical

Note: Cards displayed in this table all have the AdministrativeState equal to **Up** and a Status *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.

The columns in this table view show many attributes of each chassis.

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 113 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
- Minor

Major

Critical

Note: Interfaces displayed in this table all have the AdministrativeState equal to **Up**and a Status *other than* **Normal**.

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 **Hosted On**. 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 **Status** attribute.
Determine the types of interfaces that are being managed.	Sort on the **ifType** (interface type) attribute.
Access a map view of the network interface and its surrounding topology.	Select the interface of interest and use the **Actions** menu to select either the Layer 2 or Layer 3 Neighbor View. See Use Table Views for more information. **Tip:** You can also right-click any object in a table or map view to access the items available within the **Actions** menu.

Related Topics

Use Table Views

Export Table Information

Non-Normal Nodes View

Tip: See "Node Form" on page 65 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 **System Location**. 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 "Node Form" on page 65 and "IP Subnet Form" on page 189 for more information.
Access a map view of a selected node and its surrounding topology	Select the node of interest and use the Actions menu from the main toolbar. See Use Table Views for more information. **Tip:** You can also right-click any object in a table or map view to access the items available within the **Actions** menu.
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 168 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. Possible statuses for these nodes include:

Warning

Minor

Major

Critical

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 (SNMP 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 Addresses View

Tip: See "IP Address Form" on page 160 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

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

(*NNM iSPI Performance for Metrics*) Data appears in the **Interface Performance** view in the Monitoring workspace only if the HPE 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 113 for more details about the interface attributes that appear in this view's column headings.

Chassis Redundancy Groups View (Monitoring)

Tip: See "Chassis Redundancy Group Form" on page 270 for more details about the attributes that appear in this view's column headings.

The **Chassis Redundancy Groups** view in the Monitoring workspace is useful for identifying the names of the groups that provide redundancy protection against chassis failure.

To display the Chassis Redundancy Groups view:

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

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

   See Use Table Views for more information about sorting, filtering, and hiding attribute columns within a view.

To see the incidents related to a Chassis Redundancy Group:

1. Double-click the row representing a Chassis Redundancy Group. The "Chassis Redundancy Group Form" on page 270 displays all details about the selected Chassis Redundancy Group.
2. Navigate to the **Incidents** tab.

   A table displays the list of Incidents associated with the selected Chassis Redundancy Group.

To view the members that belong to this group:

1. Double-click the row representing a Chassis Redundancy Group. The "Chassis Redundancy Group Form" on page 270 displays all details about the selected Chassis Redundancy Group.
2. Navigate to the **Redundant Chassiss** tab.

   A table displays the list of Chassiss that belong to the selected Chassis Redundancy Group.

Related Topics:

"Chassis Redundancy Groups View (Inventory)" on page 53

Card Redundancy Groups View (Monitoring)

Tip: See "Card Redundancy Group Form" on page 274 for more details about the Card Redundancy Group attributes that appear in this view's column headings.

The **Card Redundancy Groups** view in the Monitoring workspace shows the groups of redundant cards that your network administrator configured 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. Navigate to the **Incidents** tab to see the incidents associated with the selected Card Redundancy Group.

   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.

Related Topics

Use Table Views

Export Table Information

"Card Redundancy Groups View (Inventory)" on page 53

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 279 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 279 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 293 for more details about the Node Group attributes that appear in this view's column headings.

The **Node Groups** view in the Monitoring workspace is useful for identifying the names of the groups configured by your network administrator.

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 37 for more information about filtering views using node and interface groups.

To display the Node Groups view:

1. In the **Workspaces** navigation pane, select the **Monitoring** 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 293 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, whether its status is calculated, the date and time its status was last modified, and any notes about the node group.

Custom Node Collections View

Tip: Mouse over a column heading for the complete name of a column heading attribute. See "Custom Node Collections Form" on page 307 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.

  Note: The Custom Node Collection Status is not provided for any Custom Poller Collection that has a **Collection Type** of **Bulk**.

- 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 417 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 312 for more details about the attributes that appear in the view's column headings.

Note: The **Custom Polled Instance**[1]s View is not populated for any Custom Poller Collection that has a **Collection Type** of **Bulk**.

The Custom Polled Instances view in the **Monitoring** workspace is useful for viewing the polling results for **Custom Node Collection**[2]. 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

[1]A Custom Polled Instance represents the results of a MIB variable when it is evaluated against a node. The first time a MIB variable 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.
[2]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.

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 Variable - Selected MIB variable provided by a MIB file loaded on the NNMi management server. The Custom Polled Instance represents an instance of the MIB Variable that is displayed.

  Note: Each Custom Polled Instance is associated with one instance of a MIB Variable. A MIB Variable can be associated with multiple Custom Polled Instances.

- 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. This value is used to identify the data instances that are displayed in the Line Graph. The NNMi administrator can specify the Instance Display Configuration information when configuring a MIB expression for Custom Poller.)

  Note: If the Instance Display Configuration is not set, NNMi identifies each instance that appears in a Line Graph using the Node's short DNS Name followed by the MIB Instance value in the format: <*node_name*> -<*MIB_instance_value*>. The <*node_name*> -<*MIB_instance_value*> is also used as the Display Attribute in the Custom Polled Instances view. If you are an NNMi administrator, see MIB Expressions Form (Custom Poller) for more information.

- Name of the topology Node on which the Custom Poller Policy information is being collected
- Name of the associated **Custom Node Collection**[1].
- 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.

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

[1]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.

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" below
- "Determine Problem Scope" on page 408
- "Access Node Details" on page 409

Related Topics:

Use Map Views

"Node Group Maps" on page 368

"Display the Layer 2 Neighbor View" on page 378

"Display the Layer 3 Neighbor View" on page 381

"Path Between Two Nodes that Have IPv4 Addresses" on page 382

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: • The node was just added to the NNMi database, and health status is not yet calculated. • The node is unreachable and cannot be polled.
	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.

Status Colors, continued

Color	Meaning	Description
	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	Indicates that NNMi monitoring configuration specifically excludes this device. The Status is either not calculated or the device is Not Managed/Out Of Service.
		Note: In Path View maps, note the following:
		• 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)

	Node Not Accessible	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. 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.

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 575.
- Use telnet to access the device and determine more information, see "Establish Contact with a Node (Telnet or Secure Shell)" on page 578.
- Use traceroute to view traffic paths, see "Find the Route (traceroute)" on page 577.

Note: Access to these commands depends on the **NNMi Role**[1] and Object Access Privileges to which you are assigned. If you are unable to access an action, contact your NNMi administrator.

Tip: You can also right-click any object in a table or map view to access the items available within 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 tool bar.
3. The form displays, containing details of all information related to the object.
4. View or edit the details of the selected object.

1. - **Access the Analysis Pane from a table view:**
     i. Select the workspace of interest (for example, **Inventory**).
     ii. Select the view that contains the object of interest (for example, the **Nodes** view).
     iii. Select the row that contains the object of interest.
     iv. NNMi displays detailed information at the bottom of the view in the Analysis Pane.
   - **Access the Analysis Pane in a map view:**

[1]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.

i. Select the workspace of interest (for example, **Topology Maps**).
ii. 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.

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

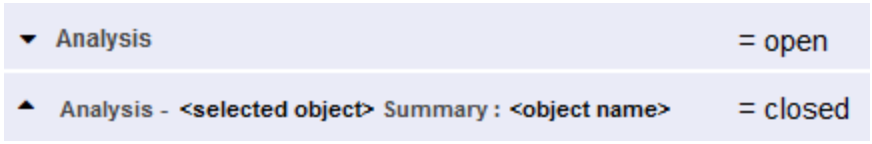
- **Access the Analysis Pane in a form:**
  - Click the form's toolbar Show Analysis icon to display information about the current form's top-level object in the Analysis Pane.

    > **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.

2. Open the Analysis Pane if necessary by clicking the expand button in the Analysis Pane banner bar:



If you change views, NNMi clears the Analysis Pane. The Analysis Pane remains blank unless an object is selected.

If you select multiple objects, the Analysis Pane displays data about the first selected object.

3. Using the Analysis Pane:
   - To resize, place your mouse cursor over the title bar to display the ↕ symbol and drag to adjust the size.
   - To refresh a subset of information in the Analysis Pane, click any displayed Refresh icon .

     To refresh all data in the Analysis Pane, open the object's form and click Refresh or Save.
   - 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.
   - 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 Sensors of type CPU, Memory, or Buffers, and Physical Sensors of type 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 *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.

- Each gauge displays the current OID value, using the default refresh rate of 15 seconds.

  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 of the *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.

- 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.

  If a gauge label appears to be a duplicate value, mouse over the label to view the more complete tooltip name that appears.

  Tip: If you are an NNMi administrator, to change the gauge title - for example, to the SNMP MIB variable name - see the "Maintaining NNMi" chapter of the *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.)

Related Topics:

"Node Form" on page 65

"Interface Form" on page 113

"IP Address Form" on page 160

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 437.

Related Topics:

Using Views to Display Data

Working with Objects

Use Table Views

Export Maps to Microsoft® Visio

Requires HPE Network Node Manager iSPI Network Engineering Toolset Software (NNM iSPI NET) -- click here for more information.

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 Map**, 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 372 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.

You can also annotate a Node Group map that is exported to Microsoft® Visio. See "Add Annotations to a Map" on page 372 for more information.

Related Topics

"Hide Connections or Connection Labels from an Exported Visio Diagram" on page 594

"View the Details for a Map Object on an Exported Visio Diagram" on the next page

"Print an Exported Visio Diagram" below

View the Details for a Map Object on an Exported Visio Diagram

Requires HPE Network Node Manager iSPI Network Engineering Toolset Software (NNM iSPI NET) -- click here for more information.

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** → **Task Panes** → **Shape Data**.

   If the object is stored in the NNMi database, NNMi displays the details available for the selected object.

Related Topics

"Export Maps to Microsoft® Visio" on page 412

"Hide Connections or Connection Labels from an Exported Visio Diagram" on page 594

"Print an Exported Visio Diagram" below

Print an Exported Visio Diagram

Requires HPE Network Node Manager iSPI Network Engineering Toolset Software (NNM iSPI NET) -- click here for more information.

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** → **Print** → **Print Preview** → **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" on page 412

"Hide Connections or Connection Labels from an Exported Visio Diagram" on page 594

"View the Details for a Map Object on an Exported Visio Diagram" above

Monitor with 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 also right-click any object in a table or map view to access the items available within the **Actions** menu.

NNMi provides a set of Line Graphs for nodes and for interfaces. See "Line Graphs Provided by NNMi" on page 422 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 to select 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.

To access a Stacked Area 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 to select the rows representing the object information.
3. Select **Tools** → **Status Distribution Graphs**.

Related Topics

"Using Line Graphs" below

"Using Stacked Area Graphs" on page 424

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.

- 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.
- 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.
- 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 Graphis restarted, the configuration changes are also displayed on any existing Line Graphs.
- The NNMi administrator determines the label that is used to identify the data instances that are displayed in Line Graphs. If the Instance Display Configuration is not set, NNMi identifies each instance that appears in a Line Graph using the Node's short DNS Name followed by the MIB Instance value in the format: *<node_name> -<MIB_instance_value>*. This value also appears as the Display Attribute in the Custom Polled Instance View. If you are an NNMi administrator, see MIB Expressions Form (Custom Poller) for more information.

From a Line Graph, you perform the following tasks:

- "Change the Lines Displayed on a Line Graph" on page 418
- "Emphasize a Line Displayed on a Line Graph" on page 420
- "Hide a Line Displayed on a Line Graph" on page 420
- "Display Messages on a Line Graph" on page 421
- "Show and Hide the Line Graph Legend" on page 422
- "Change the Polling Interval for a Graph" on page 429
- "Select a Time Segment Using the Timeline Viewer" on page 429
- "Unlock the Y-Axis When Viewing a Time Segment" on page 430
- "Change the Zoom Value for a Graph" on page 431
- "Display Data Values on a Graph" on page 431
- "Determine the Maximum Time Range for a Graph" on page 432
- "Print a Graph" on page 433
- "Export Graph Data to a Comma-Separated Values (CSV) File" on page 433

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 a 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 also right-click any object in a table or map view to access the items available within 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 416 for more information.

To display a 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 416 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. SeeAbout 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 to select each row that represents the Custom Polled Instance of interest.
3. Select **Actions** → **Graph Polled Instance** in the main toolbar.

   Tip: You can also right-click any object in a table or map view to access the items available within 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 404

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 Graphs" on page 415 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 421 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.

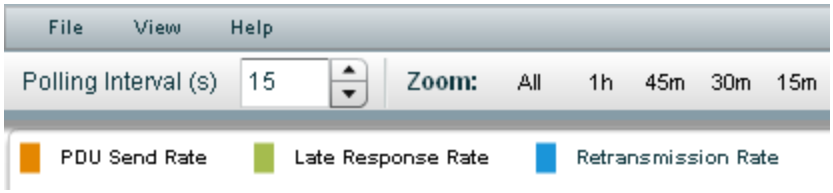
You can also choose to hide a line containing extreme values so that the Y-axis is recalculated to show more detail for the remaining lines.

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 418 for more information.

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 page 432 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:

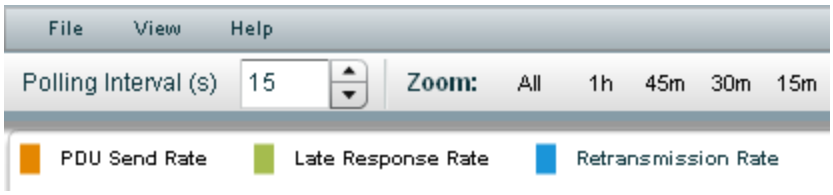
1. Select **View** → **Notification History**.
2. Do one of the following:
   - Select to clear ☐ **Show on warning** if you do not want NNMi to automatically display Warning messages in a Status pop-up window.
   - Select to check ☑ **Show on warning** to display Warning messages in a pop-up window 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.

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.

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 also right-click any object in a table or map view to access the items available within 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 to 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 to 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 page 417 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 to 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 page 418 for more information about the Line Graph displayed.

Note: You can also access Line Graphs from an object's form.

See "Monitor with Graphs" on page 415 for more information about accessing Line Graphs.

Using Stacked Area Graphs

Note: Stacked Area graphs are graphs that display data by shading the area between sets of linear data points. This graph format is only available if you have the license for an HPE Network Node Manager i Software Smart Plug-in that provides them. The HPE Network Node Manager i Software Smart Plug-in might use different terminology than Stacked Area to describe the graph.

The Stacked Area Graph enables you to view real-time SNMP data for selected objects.

Each stacked area on the graph represents a numeric value you want to monitor. If more stacked areas than the default number to be displayed on the graph are available, you can change the set of stacked areas you want to view from the default selection.

Note: If NNMi displays a gap in a stacked area on the graph, this means data was not available during the points in time indicated by the gap. Any stacked area that discontinues in the graph indicates the stacked area no longer has available data.

From a graph, you perform the following tasks:

- "Change the Stacked Areas Displayed on a Graph" below
- "Emphasize a Stacked Area Displayed on a Graph" on page 426
- "Hide Data Displayed on a Stacked Area Graph" on page 426
- "Display Messages on a Stacked Area Graph" on page 427
- "Show and Hide the Stacked Area Graph Legend" on page 428
- "Change the Polling Interval for a Graph" on page 429
- "Select a Time Segment Using the Timeline Viewer" on page 429
- "Unlock the Y-Axis When Viewing a Time Segment" on page 430
- "Change the Zoom Value for a Graph" on page 431
- "Display Data Values on a Graph" on page 431
- "Determine the Maximum Time Range for a Graph" on page 432
- "Print a Graph" on page 433

Related Topics:

Monitor Status Distribution for Network Objects

Use the Tools Menu

Change the Stacked Areas Displayed on a Graph

Stacked Area graphs are graphs that display data by shading the area between sets of linear data points. This graph format is only available if you have the license for an HPE Network Node Manager i Software Smart Plug-in that provides them. The HPE Network Node Manager i Software Smart Plug-in might use different terminology than Stacked Area to describe the graph.

When you display a Stacked Area graph, NNMi creates a stacked area for each numeric value defined for the graph.

By default, NNMi displays up to 20 stacked areas 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 stacked areas to be displayed exceeds your default number. See "Display Messages on a Stacked Area Graph" on page 427 for more information about the notification area.

Note: The NNMi administrator can change the default number of stacked areas to be initially displayed.

See the legend provided with each graph for information about the data represented by each stacked area color on the graph.

NNMi enables you to change which stacked areas are displayed in a graph.

You can also hide stacked areas displayed on a graph. When a stacked area is hidden, NNMi continues to request new data for that instance. See"Hide Data Displayed on a Stacked Area Graph" on the next page for more information.

To add a stacked area to the graph:

1. Select **File** → **Select Areas...**

   NNMi displays the Select Areas dialog box.
2. In the **Select Areas** dialog box, do one of the following:
   - To display a stacked area for one or more instances of data that appear in the Select Areas dialog box, select the check box in the row representing each instance of data that has a stacked area you want to display.
   - To display stacked areas for all instances of data that appear in the Select Areas dialog box, select the check box () that appears above the check box column.
3. Click **OK**.

   The graph displays the new set of stacked areas specified.

To remove a stacked area on the graph:

Note: If a stacked area is removed from the graph, NNMi no longer tracks the SNMP data for that instance.

1. Select **File** → **Select Areas...**

   NNMi displays the Select Areas dialog box.
2. In the **Select Areas** dialog box, do one of the following:
   - To remove a stacked area for one or more instances of data, deselect the check box () in the row representing each instance of data that has an area you want to remove.
   - To clear all stacked areas for all instances of data that appear in the Select Areas 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 graph displays the new set of stacked areas specified.

Emphasize a Stacked Area Displayed on a Graph

Stacked Area graphs are graphs that display data by shading the area between sets of linear data points. This graph format is only available if you have the license for an HPE Network Node Manager i Software Smart Plug-in that provides them. The HPE Network Node Manager i Software Smart Plug-in might use different terminology than Stacked Area to describe the graph.

NNMi enables you to emphasize a stacked area displayed in a graph.

To emphasize a stacked area on the graph:

1. Navigate to the Graph Legend.

   Note: If the Legend is not displayed, select **View** → **Show Legend**.

2. Mouse over the legend entry representing the stacked area that you want to emphasize.

   The selected legend entry appears bold and all other stacked areas fade.

Hide Data Displayed on a Stacked Area Graph

Note: Stacked Area graphs are graphs that display data by shading the area between sets of linear data points. This graph format is only available if you have the license for an HPE Network Node Manager i Software Smart Plug-in that provides them. The HPE Network Node Manager i Software Smart Plug-in might use different terminology than Stacked Area to describe the graph.

NNMi enables you to temporarily hide data displayed in a Stacked Area Graph.

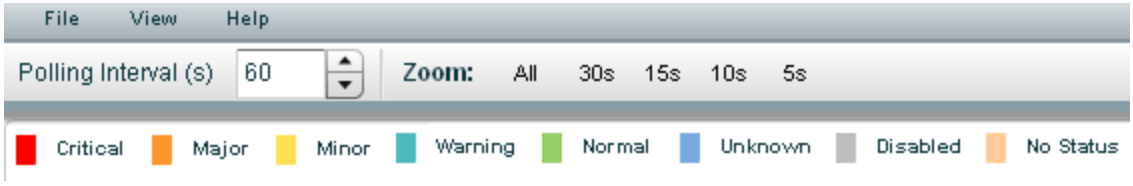
You can also choose to hide a stacked area containing extreme values so that the Y-axis is recalculated to show more detail for the remaining stacked areas.

Note: NNMi continues to request new data for instances with hidden stacked areas. A stacked area that was hidden can be added back to the graph at any time and display the most current information.

To hide a stacked area 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 stacked area that you want to hide.

3. Click the popup text to hide the line.

4. The stacked area entry disappears from the map and the Legend link text turns gray.

To display a stacked area 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 stacked area that you want to display.

3. Click the popup text display the line.

4. The stacked area entry appears on the map and the Legend link text turns black.

You can also remove a stacked area from the graph. When you remove data from the graph, NNMi stops requesting new data for that instance. See "Change the Stacked Areas Displayed on a Graph" on page 424 for more information.

Display Messages on a Stacked Area Graph

Stacked Area graphs are graphs that display data by shading the area between sets of linear data points. This graph format is only available if you have the license for an HPE Network Node Manager i Software Smart Plug-in that provides them. The HPE Network Node Manager i Software Smart Plug-in might use different terminology than Stacked Area to describe the graph.

A Stacked Area 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 stacked area 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 page 432 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.

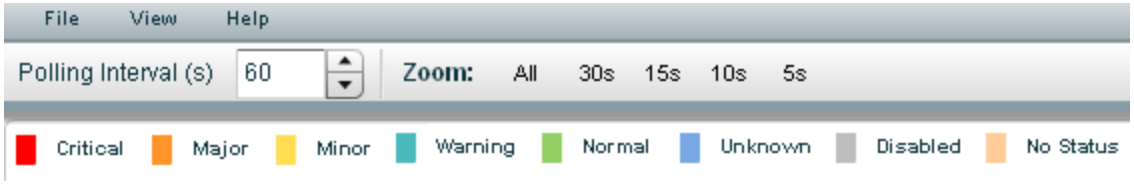
NNMi displays individual messages in a notification area that appears above the graph when a message occurs. To clear a message displayed in the notification area, click the **OK** button that appears to the right of the message. The message remains available to be displayed when using Notification History.

Show and Hide the Stacked Area Graph Legend

Note: Stacked Area graphs are graphs that display data by shading the area between sets of linear data points. This graph format is only available if you have the license for an HPE Network Node Manager i Software Smart Plug-in that provides them. The HPE Network Node Manager i Software Smart Plug-in might use different terminology than Stacked Area to describe the graph.

The Graph Legend identifies each stacked area displayed in the graph. The HPE Network Node Manager i Software Smart Plug-in determines the content and format of the Graph Legend.

NNMi enables you to temporarily hide the legend displayed in a graph. For example, if you need more than the default number of stacked areas, you might want to hide the legend to provide more space to display the graph.



To hide the legend on a graph:

Select **View** → **Show Legend**.

The check mark no longer appears next to the **Show Legend** menu option.

The legend no longer appears in the graph.

To redisplay a legend that is hidden:

Select **View** → **Show Legend**.

The check mark re-appears next to the **Show Legend** menu option.

The legend reappears in the 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.

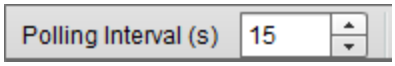
By default, NNMi uses 15 seconds, or a value specified by the NNMi administrator or HPE Network Node Manager i Software Smart Plug-in.

Note: The NNMi administrator or HPE 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 432 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.

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.

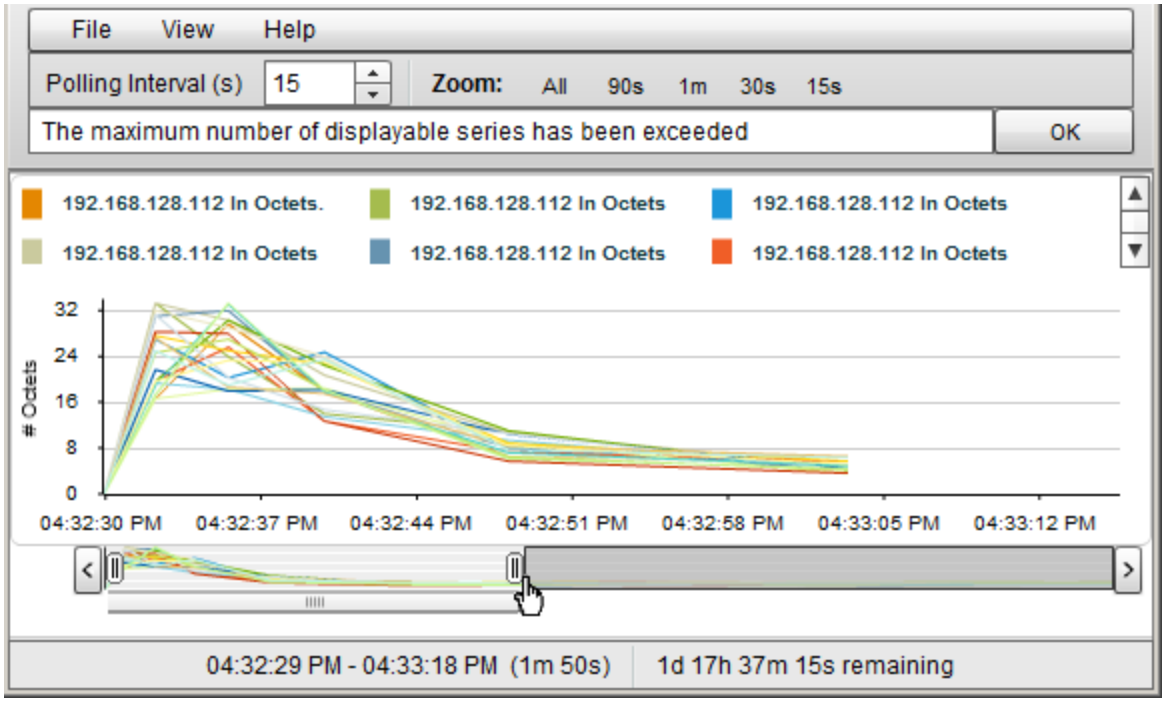
Select a Time Segment Using the Timeline Viewer

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 431 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 as 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 429 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.

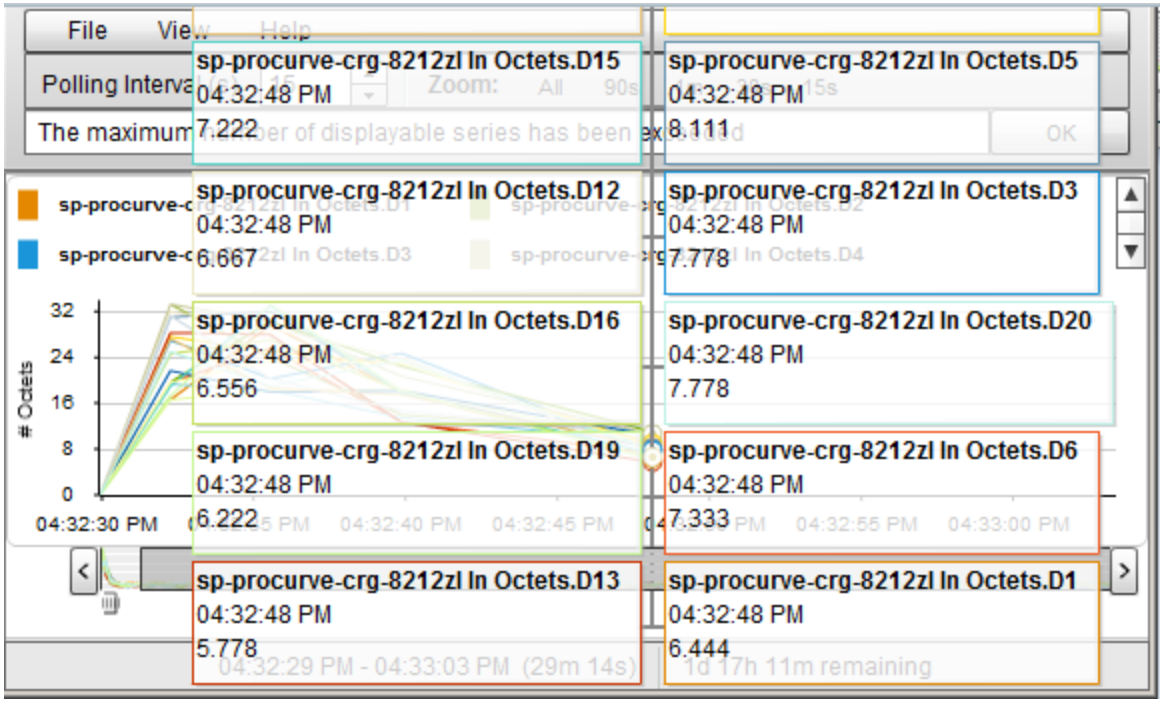
Display Data Values on a Graph

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:



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.

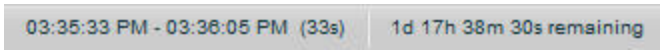
To determine the Maximum Time Range for a graph use the graph status bar. The status bar displays the following information:

- 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)



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 Graphs" on page 415.)
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.

IP Datagrams.csv

	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.

Chapter 11: Monitoring Incidents for Problems

Tip: See "Incident Form" on page 437 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 15 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. Example: 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 an is discovered and monitored (for example, node, chassis, interface, card, or address). 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	Within a view, each incident has a corresponding icon that indicates its severity so that you are immediately notified of potential or current problems. You can filter incidents so that you only view incidents 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.
Identify problem nodes	You can sort incidents by node to help you quickly identify the problem nodes.
Determine the cause of the problem	You can sort an incident view by description, to see all incidents reporting a node or interface that is disabled or otherwise unavailable. You can also use the child incidents attribute to view all of the incidents that are a result of the root cause problem reported.
Determine historical information	You can sort your incidents by notification date to determine whether a group of nodes went down within a specified time frame. You can also filter your list of incidents according to notification date to view only those incidents received within the last hour. 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. 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.
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 "Filter Views by Node or Interface Group" on page 37 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 457

"Assign Incidents" on page 458

"Unassign Incidents" on page 459

"Keep Your Incidents Up to Date" on page 460

"Track an Incident's Progress" on page 461

"Display a Map from an Incident" on page 463

Related Topics:

"Incident Views Provided by NNMi" on page 466

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 37 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 490 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	Seriousness that NNMi calculates for the incident. Possible values are: No Status Normal Warning Minor Major Critical Disabled Unknown See About Status Colors for more information about severity values. **Note:** The icons are displayed only in table views.
Priority	Used to communicate the urgency of resolving the selected incident. You control this value. NNMi sets this value to null by default. The lower the number the higher the priority. Possible values are: None Low Medium High Top **Note:** The icons are displayed only in table views.
Lifecycle State	Identifies where the incident is in the incident lifecycle. You control this value. **Registered** – Indicates that an incident arrived in the queue stored in the NNMi database.

Basic Attributes, continued

Attribute	Description
	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. 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 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 page 461 for more information about **Lifecycle State**. **Note:** The icons are displayed only in table views.
Source Node	The Name attribute value of the node associated with the incident. Click the Lookup icon and select Show Analysis or Open to display the "Node Form" on page 65 for more information about the node. **Note:** If the NNMi database does not contain any Node object for this device, the source node value is **<none>**.
Source Object	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.
Assigned To	Name of the user to which this incident is assigned. This value must be a valid user name (determined by the NNMi administrator). See "Manage Incident Assignments" on page 456 for more information.
Notes	(*NNMi Advanced - Global Network Management feature*) 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.

Basic Attributes, continued

Attribute	Description
	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. Type a maximum of 255 characters. Alpha-numeric, spaces, and special characters (~ ! @ # $ % ^ & * ( ) _+ -) are permitted. **Note:** You can sort your incident table views based on this value. Therefore, you might want to include keywords for this attribute value.

Incident Form: General Tab

The "Incident Form" on page 437 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	Generated by NNMi to indicate the problem category. Possible values include: **Accounting** - 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. **Application Status** - 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. **Configuration** - Indicates there is a problem with the configuration of a managed device. For example, there is a physical address mismatch. **Fault** – Indicates a problem with the network; for example, Node Down. **Performance** – Indicates an exceeded threshold. For example, a utility exceeds 90 percent. **Security** – Indicates there is a problem related to authentication; for example, an SNMP authentication failure. **Status** - Often indicates some status change occurred on a device. For example, when a Cisco device powers up or powers down. **Note:** The icons are only in table views.

General Attributes, continued

Attribute	Description
Family	Used to further categorize the types of incidents that might be generated. Possible values are: **Address** – Indicates the incident is related to an address problem. **Aggregated Port** – Indicates the incident is related to a **Link Aggregation**[1] or **Split Link Aggregation**[2] problem. See "Interface Form: Link Aggregation Tab (NNMi Advanced)" on page 121. **BGP** - 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. **Card** – Indicates the incident is related to an card problem. This family is not used by NNMi with default configurations, but it is available for incidents you define. **Chassis** – 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. **Component Health** – Indicates the incident is related to Node Sensor or Physical Sensor data collected by NNMi. See Chassis Form: Physical Sensors Tab and Card Form: Physical Sensors Tab for more information. **Connection** – Indicates the incident is related to a problem with one or more connections. **Correlation** – 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. **Custom Poller** – Indicates the incident is related to the NNMi Custom Poller feature. See About Custom Poller. **DLCI** – Indicates the incident is related to a problem with one or more DLCI connections. **HSRP** – (*NNMi Advanced*) Indicates the incident is related to a Hot Standby Router Protocol (**HSRP**[3]) problem. **IP Subnet** – Indicates the incident is related to a subnet problem. **Interface** – Indicates the incident is related to a problem with one or more interfaces. **License** - Indicates the incident is related to a licensing problem.

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.
[3]Hot Standby Router Protocol

General Attributes, continued

Attribute	Description
	NNMi Health – Indicates the incident is related to NNMi Health. See the Check NNMi Health for more information. **Node** – Indicates the incident is related to a node problem. **OSPF** – 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. **RAMS** – (*HPE Route Analytics Management System (RAMS) for MPLS WAN*) Indicates the incident is related to a Router Analytics Management System problem. If you are an NNMi administrator, see HPE RAMS MPLS WAN Configuration (NNMi Advanced) for information about configuring RAMS. **RMON** – 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. **RRP** – (*NNMi Advanced*) Indicates the incident is related to a Router Redundancy Protocol configuration problem. **STP** – 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. **Stack** – Indicates the incident is related to an stack problem. This family is not used by NNMi with default configurations, but it is available for incidents you define. **Syslog** – NNMi does not use this Family with default configurations. It is available for incidents you define. **System and Applications** – Indicates the incident is related to a problem with one or more systems or applications. **Trap Analysis** – (*HPE Network Node Manager iSPI Network Engineering Toolset Software*) Indicates the incident is related to an SNMP trap storm. **VLAN** – Indicates the incident is related to a problem with a virtual local area network. **VRRP** – (*NNMi Advanced*) Indicates the incident is related to a Virtual Router Redundancy Protocol (**VRRP**[1]) problem.
Origin	Identifies how the incident was generated. Possible values are: **NNMi** – Indicates the incident was generated by NNMi processes. **Manually Created** – NNMi does not use this Origin with default configurations. It is available for incidents you define. **SNMP Trap** – Indicates the incident was forwarded from an SNMP Agent.

[1]Virtual Router Redundancy Protocol

General Attributes, continued

Attribute	Description
	Syslog – NNMi does not use this Origin with default configurations. It is available for incidents you define. **Other** – Indicates the incident was generated by a source other than the Origin categories provided.
Correlation Nature	This incident's contribution to a root-cause calculation, if any. Possible values are: **Root Cause** – Indicates the Incident is determined by NNMi's Causal Engine to be the source of a problem (for example, Node Down). **User Root Cause** – Indicates the Incident is configured by your NNMi administrator to make NNMi always treats this Incident as Correlation Nature: Root Cause. **Secondary Root Cause** – 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. For example, if an **Interface Down** incident is followed by a **Node Down** Incident on a neighboring device, the **Interface Down** Incident becomes a Child Incident to the Parent **Node Down** incident. Its Correlation Nature becomes Secondary Root Cause. 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. **Symptom** – 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 **Symptom** to an Interface Down incident in the root cause incidents view. **Service Impact** - 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 HPE Network Node Manager i Software Smart Plug-ins (iSPIs). See "Help for Administrators" for more information about NNM iSPIs. **None** – Indicates there is no incident correlation for the incident. **Info** – Indicates the incident is informational only. **Dedup Stream Correlation** – Stream correlations are created as NNMi analyzes events and traps to determine the root cause incident for a problem.

General Attributes, continued

Attribute	Description
	Dedup Stream Correlation indicates the Incident is a Deduplication Incident. 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. **Rate Stream Correlation** – 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. Rate Incidents track incident patterns *based on the number of incident reoccurrences within a specified time period*. 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.
Duplicate Count	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. 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 **Duplicate Count** value. Note the following: • By default, NNMi updates the **Duplicate Count** every 30 seconds. This interval cannot be changed. • 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. See "About the Incident Lifecycle" on page 461 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. • Duplicates are configured by the NNMi administrator using the **SNMP Trap Configuration, Syslog Messages Configuration**, or **Management Event Configuration** form available from the **Configuration** workspace.
RCA Active	Used by NNMi to identify whether NNMi considers the incident to be active or inactive. If set to **True**, the incident is considered to be active. If set to **False**, the incident is considered to be inactive. NNMi considers an incident to be active when the root cause analysis (RCA) engine is actively evaluating the problem reported by this incident.

General Attributes, continued

Attribute	Description
	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. NNMi initially sets an incident's **RCA Active** attribute to True and the incident's Lifecycle State to **Registered**. When NNMi sets the **RCA Active** attribute to **False**, it also sets the incident's Lifecycle State to **Closed**. Examples of when an incident's **RCA Active** attribute is set to **False** include: • When an interface goes up, NNMi closes the InterfaceDown incident. • When a node goes up, NNMi closes the NodeDown incident.
Correlation Notes	Stores notes about the correlation status of the 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.
First Occurrence Time	Used when suppressing duplicate incidents or when specifying an incident rate. Indicates the time when the duplicate or rate criteria were first met for a set of duplicate incidents or for a set of incidents that has a rate criteria that was met.
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 437 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 437 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 437 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	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. 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.

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 437 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	Name used to identify the CIA. The Custom Incident Attribute (CIA) name limit is 80 characters. If this limit is exceeded, NNMi truncates the value from the left. **Note:** 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
Type	Describes the type of data that is stored for the CIA. Examples of types include:

Custom Incident Attributes, continued

Attribute	Description
	Double - Used to describe real numbers; for example 12.3 **Integer** - Used for integer numeric values; for example 1, 2, or 3 **String** - Used for character values **Boolean** - Used to store true or false values **Note:** All SNMP Trap types begin with **asn**. If the CIA represents a varbind value, NNMi might provide additional types, such as **Counter**.
Value	For management events that are generated from NNMi, this value is the CIA value in the incident that was provided by NNMi. The Custom Incident Attribute value limit is 2000 characters. If this limit is exceeded, NNMi truncates the value from the right.

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 437, 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	The time measured in milliseconds between when NNMi detected a problem with one or more network devices to the time the problem was resolved. **Note:** 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

Custom Incident Attributes Provided by NNMi, continued

Name	Description
	include cia.incidentDurationMs.
cia.reasonClosed	The Conclusion information identifying the reason NNMi changed the incident's Lifecycle State to Closed. For example, NNMi might include an Interface Up Conclusion as the reason an Interface Down incident was closed. **Note:** This CIA is used when NNMi's Causal Engine has analyzed and Closed the incident. Software that is integrated with NNMi might also provide values for cia.reasonClosed. Any time an incident is closed manually (for example, by the network operator), NNMi does not include cia.reasonClosed.
cia.remotemgr	(*NNMi Advanced - Global Network Management feature*) Hostname or IP address of the either of the NNMi Regional Manager that is forwarding the event.
cia.snmpoid	SNMP trap object identifier.
cia.timeIncidentDetectedMs	The timestamp in milliseconds when NNMi first detected the problem on the network device associated with the incident. **Note:** 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.timeIncidentDetectedMs.
cia.timeIncidentResolvedMs	The time when NNMi determines the problem on the network device associated with the incident is resolved. **Note:** 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.

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	The monitored attribute that is being measured. The NNMi administrator

Custom Incident Attributes Provided for Fault Thresholds and Performance Thresholds, continued

Name	Description
	configures these thresholds. Possible threshold values for Nodes include: • 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

Custom Incident Attributes Provided for Fault Thresholds and Performance Thresholds, continued

Name	Description
	compared to the total amount of available memory. • 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*) Possible performance thresholds for Interfaces include: Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information. • FCS LAN Error Rate *Local Area Network interfaces only*.Threshold based on the percentage of incoming frames with a bad checksum (**CRC**[1] value) compared to the total number of incoming frames. Possible causes include collisions at half-duplex, a duplex mismatch, bad hardware (**NIC**[2], 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**[3] value) compared to the total number of incoming frames. Possible causes include wireless communication interference, bad hardware (**NIC**[4], 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

[1]Cyclic Redundancy Check
[2]Network Interface Controller
[3]Cyclic Redundancy Check
[4]Network Interface Controller

Custom Incident Attributes Provided for Fault Thresholds and Performance Thresholds, continued

Name	Description
	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 as collisions and buffer errors.

Custom Incident Attributes Provided for Fault Thresholds and Performance Thresholds, continued

Name	Description
	• 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.
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 **Nominal** to **High**, based on a change in the thresholdMeasuredValue. See Interface Form for a complete list of possible values.
cia.thresholdCurrentValue	Results from the most recent Fault Polling Interval or Performance Polling Interval. For example, **High**. See Interface Form 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 447

Incident Form: Diagnostics Tab

The "Incident Form" on page 437 provides details for troubleshooting purposes.

For information about each tab:

Diagnostics Table

Attribute	Description
List of Diagnostics	Requires HPE Network Node Manager iSPI Network Engineering Toolset Software (NNM iSPI NET) and requires installation of a Diagnostic Server -- click here for more information. The history of all the Diagnostic reports that have been run for the incident's Source Node. Diagnostics are sets of automated commands specific to one or more device types, including Cisco routers and switches, Cisco switch/routers, and Nortel switches. To generate a new instance of these Diagnostics reports, click **Actions** → **Run Diagnostics**. **Tip:** You can also right-click any object in a table or map view to access the items available within the **Actions** menu. Double-click the row representing a Diagnostic report. NNMi displays all details about the selected report. See "Incident Diagnostic Results Form (Flow Run Result)" below.

Incident Diagnostic Results Form (Flow Run Result)

Requires HPE Network Node Manager iSPI Network Engineering Toolset Software (NNM iSPI NET) and requires installation of a Diagnostic Server -- click here for more information.

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

Tip: You can also right-click any object in a table or map view to access the items available within 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" above 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	The current status of this NNM iSPI NET Diagnostics report. Possible values include: **New** - The Diagnostic is in the queue, but is not yet running **In Progress** -The Diagnostic has been submitted and is not finished running **Completed** - The Diagnostic has finished running **Not Submitted** - An error condition prevented the Diagnostic from being submitted **Timed Out** - 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. Example error conditions include the following: • The number of Diagnostics in the queue might prevent NNMI from submitting the Diagnostic. • A configuration error, such as an incorrect user name or password, might prevent NNMi from accessing the required Operations Orchestration server. Contact your NNMi administrator for Diagnostic log file information.
Report	NNM iSPI NET uses this text string to display the selected instance of the diagnostics report in a browser window. Click this link to open the actual report. **Note:** You might be prompted to provide a user name and password to access the Operations Orchestration software. See the *NNM iSPI NET Planning and Installation Guide* for more information.
Lifecycle State	Incident Lifecycle State of the target Incident. If the incident's Lifecycle State matches the value specified here, the Diagnostic runs. 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).
Last Update Time	Date and time NNM iSPI NET last updated this instance of the Diagnostics report. NNM iSPI NET uses the locale of the client and the date and time from the NNMi management server.

Incident Form: Registration Tab

The "Incident Form" on page 437 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. **Note:** This value does not change when a node is rediscovered. This is because the Node object is modified, but not created.
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. Note the following: • 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. • 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.

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 also right-click any object in a table or map view to access the items available within the **Actions** menu.

Tasks Related to Assigning Incidents

Task	How	Required Minimum NNMi User Role
Own an incident	Select an incident and use **Actions** → **Assign** →**Own Incident**. See "Own Incidents" below for more information.	Level 1 Operator (with more limited access privileges than Level 2 Operators)
Assign an incident to someone else	There are two ways to assign an incident to someone else (see "Assign Incidents" on the next page for more information): • From any Incident view, select one or more Incidents and use **Actions** → **Assign** → **Assign Incident**. • From an Incident form, use **Actions** → **Assign** → **Assign Incident**.	Level 1 Operator
Un-assign an incident	Select an incident and use **Actions** → **Assign** → **Unassign Incident**. See "Unassign Incidents" on page 459 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 to select each row that represents an incident you want to own.
3. Select **Actions** → **Assign** → **Own Incident**.

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

Your user name appears in the **Assigned To** column in any incident views that include the incident.

Note the following:

- Your NNMi administrator might have configured the **Assigned To** value to show a display name that consists of one or more Lightweight Directory Access Protocol (LDAP) properties rather than the user name assigned to NNMi. When configured to show display names, NNMi filters and sorts on the stored user name value, but shows the display name in the Incidents table. If you are an NNMi administrator, see the "Maintaining NNMi" chapter in the HPE Network Node Manager i Software Deployment Reference for more information.

- 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 468 for more information.

Assign Incidents

If you are an NNMi user with a Level 1 Operator (with more limited 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 15 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 also right-click any object in a table or map view to access the items available within the **Actions** menu.
3. Select the user name.

   Your NNMi administrator might have configured the **Assigned To** value to display one or more Lightweight Directory Access Protocol (LDAP) properties rather than the name used to sign in to NNMi. If you are an NNMi administrator, see the "Maintaining NNMi" chapter in the HPE Network Node Manager i Software Deployment Reference for more information.
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 471 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 to select each row that represents an incident you want to assign.
3. Select **Actions** → **Assign** → **Assign Incident**.
4. Select the user name.

   Your NNMi administrator might have configured the **Assigned To** value to display one or more Lightweight Directory Access Protocol (LDAP) properties rather than the name used to sign in to NNMi. If you are an NNMi administrator, see the "Maintaining NNMi" chapter in the HPE Network Node Manager i Software Deployment Reference for more information.

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 471 for more information.

Unassign Incidents

If you are an NNMi user with a user role of Level 1 Operator (with more limited 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 also right-click any object in a table or map view to access the items available within 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 471 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 to 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 471 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 1024 characters. Alpha-numeric, spaces, and special characters are permitted.
4. 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 the next page 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" below.

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.

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 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 also right-click any object in a table or map view to access the items available within 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 also right-click any object in a table or map view to access the items available within 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: The current values of the management mode attributes (**Managed**/ **Not Managed** / **Out of Service**) determine whether NNMi discovers an object. Map symbols with the color set to the following are not currently being monitored:
No Status

Related Topics:

Use Map Views

"Display the Layer 2 Neighbor View" on page 378

"Display the Layer 3 Neighbor View" on page 381

"Path Between Two Nodes that Have IPv4 Addresses" on page 382

"Node Group Overview Map" on page 374

"Routers Map" on page 377

"Switches Map" on page 378

"Networking Infrastructure Devices Map" on page 376

"Display a Line Graph from an Incident (Custom Poller Only)" on page 417

"Understand the Effects of Setting the Management Mode to Not Managed or Out of Service" on page 589

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 also right-click any object in a table or map view to access the items available within 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 also right-click any object in a table or map view to access the items available within 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 480.

   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 480.

   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 417

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 SNMP Trap Incidents to the Global Manager:

On the Global Manager, the **Custom Incident Attribute** tab on the Incident form identifies if the SNMP Trap Incident 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 Regional Manager.
   - If `cia.remotemgr` appears in the list of Custom Attributes, NNMi displays the hostname of the NNMi Regional Manager 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 Incident 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 470
- "Unassigned Open Key Incidents View" on page 471
- "My Open Incidents View" on the next page
- "Closed Key Incidents View" on page 472
- "Open Root Cause Incidents View" on page 474
- "Service Impact Incidents View" on page 475
- "All Incidents View" on page 475
- "Custom Open Incidents View" on page 476
- "Custom Incidents View" on page 477
- "SNMP Traps View" on page 479

The most useful views for proactively monitoring your network for problems are the **Key Incident**[1] views (see "Key Incident Views" on the next page). 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 views available in 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.

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

Other useful tasks from the incident view, include the following:

- "Display a Map from an Incident" on page 463
- "Node Form" on page 65

Related Topics:

About Workspaces

About the NNMi Console

[1]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.

My Open Incidents View

Tip: See "Incident Form" on page 437 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 in the Incident Management workspace 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** 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 435 for more information about ways to use incident views.

Key Incident Views

Tip: See "Incident Form" on page 437 for more details about the incident attributes that appear in a key incident view's column headings.

The **Key Incident**[1] 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:

[1]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.

- Severity is *other than* Normal.
- Correlation Nature is any of the following:

Incident Correlation Nature	Description
Info	This Correlation Nature is meant to be informational.
None	Indicates there is no incident correlation for this incident.
Rate Stream Correlation	Indicates the incident tracks incident patterns *based on the number of incident reoccurrences within a specified time period*. 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.
Root Cause	Indicates an incident that NNMi's Causal Engine determined to be the root cause of a problem.
User Root Cause	Indicates that your NNMi administrator configured NNMi to always treat this Incident as Correlation Nature: Root Cause.

Note: Key Incidents do not include Incidents with following Correlation Natures because they are not considered to be Key Incidents:

Dedup Stream Correlation

Secondary Root Cause

Symptom

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" on the next page

NNMi provides the following Key Incident view filtered to display lifecycle state value of **Closed**:

- "Open Key Incidents View" on the next page"Closed Key Incidents View" on page 472

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 page 471

Related Topics

Use Table Views

"Organize Your Incidents" on page 437

"Monitoring Incidents for Problems" on page 435

"Display a Map from an Incident" on page 463

Open Key Incidents View

Tip: See "Incident Form" on page 437 for more details about the incident attributes that appear in this view's column headings.

The **Open Key Incidents** view in the Incident Browsing workspace and Incident Management workspace shows the incidents that are most important to network Operators and that often require more immediate action. This view displays any **Key Incident**[1] 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**[2] 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** or **SNMP Trap**), its **Correlation Nature** (for example, **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.
- Your NNMi administrator might have configured the **Assigned To** value to show a display name that consists of one or more Lightweight Directory Access Protocol (LDAP) properties rather than the user name assigned to NNMi. When configured to show display names, NNMi filters and sorts on the stored user name value, but shows the display name in the Incidents table. If you are an NNMi administrator, see the "Maintaining NNMi" chapter in the HPE Network Node Manager i Software Deployment Reference for more information.

See "Monitoring Incidents for Problems" on page 435 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

[1] 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.
[2] 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.

"Organize Your Incidents" on page 437

"Monitoring Incidents for Problems" on page 435

"Display a Map from an Incident" on page 463

"Key Incident Views" on page 468

"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 437 for more details about the incident attributes that appear in this view's column headings.

The **Unassigned Open Key Incident** view in the Incident Management workspace displays any **Key Incident**[1] 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** or **SNMP Trap**), its Correlation Nature (for example, **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 435 for more information about ways to use incident views.

Related Topics

Use Table Views

"Organize Your Incidents" on page 437

"Monitoring Incidents for Problems" on page 435

"Display a Map from an Incident" on page 463

"Key Incident Views" on page 468

[1]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.

"Open Key Incidents View" on page 470

"Closed Key Incidents View" below

Closed Key Incidents View

Tip: See "Incident Form" on page 437 for more details about the incident attributes that appear in this view's column headings.

The **Closed Key Incidents** view in the Incident Browsing workspace displays any **Key Incident**[1] 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**[2] views.

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** 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.
- Your NNMi administrator might have configured the **Assigned To** value to show a display name that consists of one or more Lightweight Directory Access Protocol (LDAP) properties rather than the user name assigned to NNMi. When configured to show display names, NNMi filters and sorts on the stored user name value, but shows the display name in the Incidents table. If you are an NNMi administrator, see the "Maintaining NNMi" chapter in the HPE Network Node Manager i Software Deployment Reference for more information.

See "Monitoring Incidents for Problems" on page 435 for more information about ways to use incident views.

[1]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.
[2]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.

Related Topics:

Use Table Views

"Organize Your Incidents" on page 437

"Monitoring Incidents for Problems" on page 435

"Display a Map from an Incident" on page 463

"Key Incident Views" on page 468

"Open Key Incidents View" on page 470

"Unassigned Open Key Incidents View" on page 471

Root Cause Incidents

Tip: See "IP Address Form" on page 160"Incident Form" on page 437 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 the management protocols available (for example 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 519
- "Interface Down" on page 512
- "Address Not Responding" on page 491

NNMi provides the "Open Root Cause Incidents View" on the next page

Tip: When using Incident views:

- **Root Cause** value = determined by NNMi's Causal Engine
- **User Root Cause** = your NNMi administrator configured NNMi to always treat this Incident as Correlation Nature: Root Cause

See "Monitoring Incidents for Problems" on page 435 for more information about ways to use incident views.

Related Topics:

Use Table Views

"Organize Your Incidents" on page 437

"Monitoring Incidents for Problems" on page 435

"Display a Map from an Incident" on page 463

Open Root Cause Incidents View

Tip: See "Incident Form" on page 437 for more details about the incident attributes that appear in this view's column headings.

The **Open Root Cause Incidents** view in the Incident Browsing workspace 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 CauseIncidents 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** 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.
- Your NNMi administrator might have configured the **Assigned To** value to show a display name that consists of one or more Lightweight Directory Access Protocol (LDAP) properties rather than the user name assigned to NNMi. When configured to show display names, NNMi filters and sorts on the stored user name value, but shows the display name in the Incidents table. If you are an NNMi administrator, see the "Maintaining NNMi" chapter in the HPE Network Node Manager i Software Deployment Reference for more information.

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 also right-click any object in a table or map view to access the items available within the **Actions** menu.

Related Topics:

Use Table Views

"Organize Your Incidents" on page 437

"Monitoring Incidents for Problems" on page 435

"Display a Map from an Incident" on page 463

"Unassigned Open Key Incidents View" on page 471

"Closed Key Incidents View" on page 472

Service Impact Incidents View

Tip: See "Incident Form" on page 437 for more details about the incident attributes that appear in this view's column headings.

The **Service Impact Incidents** view in the Incident Browsing workspace 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 HPE 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.
- Your NNMi administrator might have configured the **Assigned To** value to show a display name that consists of one or more Lightweight Directory Access Protocol (LDAP) properties rather than the user name assigned to NNMi. When configured to show display names, NNMi filters and sorts on the stored user name value, but shows the display name in the Incidents table. If you are an NNMi administrator, see the "Maintaining NNMi" chapter in the HPE Network Node Manager i Software Deployment Reference for more information.

See "Monitoring Incidents for Problems" on page 435 for more information about ways to use incident views.

All Incidents View

Tip: See "Incident Form" on page 437 for more details about the incident attributes that appear in this view's column headings.

The **All Incidents** view in the Incident Browsing workspace 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**, 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.
- Your NNMi administrator might have configured the **Assigned To** value to show a display name that consists of one or more Lightweight Directory Access Protocol (LDAP) properties rather than the user name assigned to NNMi. When configured to show display names, NNMi filters and sorts on the stored user name value, but shows the display name in the Incidents table. If you are an NNMi administrator, see the "Maintaining NNMi" chapter in the HPE Network Node Manager i Software Deployment Reference for more information.

See "Monitoring Incidents for Problems" on page 435 for more information about ways to use incident views.

Custom Open Incidents View

Tip: See "Incident Form" on page 437 for more details about the incident attributes that appear in this view's column headings.

The **Custom Open Incidents** view in the Incident Browsing workspace 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** 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.
- Your NNMi administrator might have configured the **Assigned To** value to show a display name that consists of one or more Lightweight Directory Access Protocol (LDAP) properties rather than the user name assigned to NNMi. When configured to show display names, NNMi filters and sorts on the stored user name value, but shows the display name in the Incidents table. If you are an NNMi administrator, see the "Maintaining NNMi" chapter in the HPE Network Node Manager i Software Deployment Reference for more information.

See Filter a Table View for more information about how to filter information displayed in a table.

See "Monitoring Incidents for Problems" on page 435 for more information about ways to use incident views.

See "Incident Form" on page 437 for more information about incident attributes.

Related Topics:

Use Table Views

"Organize Your Incidents" on page 437

"Display a Map from an Incident" on page 463

Custom Incidents View

Tip: See "Incident Form" on page 437 for more details about the incident attributes that appear in this view's column headings.

The **Custom Incidents** view in the Incident Browsing workspace 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** 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.
- Your NNMi administrator might have configured the **Assigned To** value to show a display name that consists of one or more Lightweight Directory Access Protocol (LDAP) properties rather than the user name assigned to NNMi. When configured to show display names, NNMi filters and sorts on the stored user name value, but shows the display name in the Incidents table. If you are an NNMi administrator, see the "Maintaining NNMi" chapter in the HPE Network Node Manager i Software Deployment Reference for more information.

See Filter a Table View for more information about how to filter information displayed in a table.

See "Monitoring Incidents for Problems" on page 435 for more information about ways to use incident views.

See "Incident Form" on page 437 for more information about incident attributes.

Related Topics:

Use Table Views

"Organize Your Incidents" on page 437

"Display a Map from an Incident" on page 463

Syslog Messages View (HPE ArcSight)

Tip: See "Incident Form" on page 437 for more details about the incident attributes that appear in this view's column headings.

The HPE 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 also right-click any object in a table or map view to access the items available within 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 437 for more details about the incident attributes that appear in this view's column headings.

The **SNMP Traps** view in the Incident Browsing workspace 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 12: 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 490 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 Node Sensors: for example buffers. CPU, disks, memory)
  - Chassis (and Physical Sensors: for example backplane, fan, power, temperature, voltage)
  - Card
  - Interface
  - IP Address
  - SNMP Agent
  - Node Group
  - Card Redundancy Group
  - Router Redundancy Group
- 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 associated with the object by selecting **Open** using the Lookup icon from the **Hosted on Node** or **Managed By** attribute.

  Once again, information about the State, Status, and Conclusions can assist yow 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 485
  - "View the Monitoring Settings Report" on page 486
  - "Verify Current Status of a Device" on page 488
- 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 573
  - "Test Node Access (Ping)" on page 575
  - "Find the Route (traceroute)" on page 577
  - "Establish Contact with a Node (Telnet or Secure Shell)" on page 578
  - "Check Status Details for a Node Group" on page 579

  Note: You can also access Line Graphs from the **Actions** menu to investigate a problem. See "Monitor with Graphs" on page 415 for more information.
- Use **Tools → MIB Browser** or select **Actions → MIB Information → MIB Browser** from a Node or Incident form to view MIB Information for a node. See "Run SNMP Walk Commands (MIB Browser)" on page 351 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 also right-click any object in a table or map view to access the items available within 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 569
  - "Find the Attached Switch Port" on page 571
  - "Checking the Status of NNMi" on page 594

Use a Dashboard View

To begin diagnosing a problem, you might want to view current information about the object.

NNMi includes dashboard views, which can contain multiple panels of data pertaining to the entire network, a specific object (for example, a node or interface), or a group of objects (such as a Node Group or Interface Group).

Dashboard views provide at-a-glance information, allowing you to easily compare and quickly isolate the information you need to analyze data and diagnose problems. Dashboard panels might contain a variety of tables and charts, some of which might are customizable.

There are two types of dashboard views:

- Views available in the Dashboards Workspace
- Dashboard Views based on an Object

Related Topics for NNM iSPI Performance Dashboard Data:

"Performance Analysis with Additional Views" on page 57

"Node Performance Metrics" on page 57

"Interface Performance Metrics" on page 59

Use Dashboard Views

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.

1. - **Access the Analysis Pane from a table view:**
     i. Select the workspace of interest (for example, **Inventory**).
     ii. Select the view that contains the object of interest (for example, the **Nodes** view).
     iii. Select the row that contains the object of interest.
     iv. NNMi displays detailed information at the bottom of the view in the Analysis Pane.
   - **Access the Analysis Pane in a map view:**
     i. Select the workspace of interest (for example, **Topology Maps**).
     ii. 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.

iii. Click the map object of interest.

iv. NNMi displays detailed information at the bottom of the view in the Analysis Pane.

- **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.

2. Open the Analysis Pane if necessary by clicking the expand button in the Analysis Pane banner bar:

If you change views, NNMi clears the Analysis Pane. The Analysis Pane remains blank unless an object is selected.

If you select multiple objects, the Analysis Pane displays data about the first selected object.

3. Using the Analysis Pane:
   - To resize, place your mouse cursor over the title bar to display the ↕ symbol and drag to adjust the size.
   - To refresh a subset of information in the Analysis Pane, click any displayed Refresh icon .

     To refresh all data in the Analysis Pane, open the object's form and click Refresh or Save.
   - 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.
   - 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 Sensors of type CPU, Memory, or Buffers, and Physical Sensors of type 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 *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.

- Each gauge displays the current OID value, using the default refresh rate of 15 seconds.

  > **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 of the *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.

- 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.

  If a gauge label appears to be a duplicate value, mouse over the label to view the more complete tooltip name that appears.

  > **Tip:** If you are an NNMi administrator, to change the gauge title - for example, to the SNMP MIB variable name - see the "Maintaining NNMi" chapter of the *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.)

> **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	• Summary panel • Interface information and analysis • IP address information and analysis • SNMP information
Interface	• Summary panel • IP address information and analysis
Incidents	• Summary panel

Examples of Possible Analysis Pane Information, continued

Object	Possible Analysis Information
	• Source Node information and analysis • Source Object information and analysis

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 also right-click any object in a table or map view to access the items available within

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 also right-click any object in a table or map view to access the items available within 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 *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.

(*NNM iSPI Performance for Metrics*) The HPE 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 About Node and Interface Groups for more information.
Fault Polling (SNMP and ICMP)	If enabled, State Poller monitors all managed interfaces, IP addresses, and SNMP agents by issuing ICMP pings and SNMP read-only queries for MIB-II `ifAdminStatus` and `ifOperStatus`.

Monitoring Possibilities, continued

Attribute	Description
	(`ifAdminStatus` is set by the device administrator. `ifOperStatus` indicates the overall health of the device and is supplied by the SNMP Agent.) If disabled: • Devices that were already discovered remain with the last calculated state/status. • Newly discovered devices are set to "No Status" with map-symbol background shape color set to beige.
Fault Polling Interval	The time that State Poller waits between issuing queries to gather fault information. The default Fault Polling Interval is 5 minutes, except for the Node Group named Microsoft Windows Systems which is 10 minutes.
Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.	
Performance Polling	(*NNM iSPI Performance for Metrics*) If enabled, the HPE 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. If disabled, network performance data is not currently available.
Performance Polling Interval	(*NNM iSPI Performance for Metrics*) The time that the HPE Network Node Manager iSPI Performance for Metrics Software waits between issuing queries to gather performance information. The default Performance Polling Interval is 5 minutes, except for the Node Group named Microsoft Windows Systems which is 10 minutes.

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 Sensor:

1. Navigate to a Node view (for example, **Inventory** workspace, **Node Sensors** view).
2. Select the Node Sensor of interest by selecting the row representing the object information.
3. Select **Actions** → **Configuration Details** → **Monitoring Settings**.

Note: This menu item is also available on any **Node Sensors** form.

To view the monitoring configuration for a Physical Sensor:

1. Navigate to a Node view (for example, **Inventory** workspace, **Physical Sensors** view).
2. Select the Physical Sensor of interest by selecting the row representing the object information.
3. Select **Actions** → **Configuration Details** → **Monitoring Settings**.

Note: This menu item is also available on any **Physical Sensors** form.

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 also right-click any object in a table or map view to access the items available within 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 to 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 to 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: • If the target is responding. • If the poll was successful. • How long it took to get an answer.
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 62. Check the information displayed on the "Node Form: Status Tab" on page 93 and the "Node Form: Node Sensors Tab" on page 84.
- Check the Node icon status colors on maps ("Watch Status Colors" on page 406).
- 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 437 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 480 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 519)
- A node or connection might be down and need your attention (see "Node or Connection Down" on page 515)
- An interface is operationally down (see "Interface Down" on page 512)
- 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 507)

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 437 displays all details about the selected incident.

The **SNMP Trap Incident Configuration** or **Management Event Incident 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 406 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 **AddressNotResponding** Conclusion.
Incident	Adds the **Address Not Responding** incident. Incident Name: `AddressNotResponding`
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

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 **Critical**.
Status	Adds the **Minor** Status.
Conclusion	**SomeUnresponsiveAddressesInNode** **Note:** If you view an **AllUnresponsiveAddressesInNode** Conclusion, see "Node Down" on page 519 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 440 for more information.
- The Node Status is changed to **Normal**. The Conclusion on the Node is ResponsiveAddressInNode.

Aggregator Interface Degraded (*NNMi Advanced*)

Link Aggregation[1] or **Split Link Aggregation**[2]: 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 **AggregatorDegraded** Conclusion.
Incident	Adds the **Aggregator Interface Degraded** incident. Incident Name: `AggregatorDegraded` The **Correlated Children** tab has an **Interface Down** incident for the member interfaces that have a Status of **Critical**. Incident Name: `InterfaceDown`
Status	Adds the **Minor** Status.
Overall Status	Changes to **Minor**.

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 **Critical**.

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

Source Node Updates, continued

Tab	Description
Status	Adds the **Minor** Status.
Conclusions	**InterfacesDownInNode**

See "Interface Down" on page 512 for more information about Interface Down incidents.

On Layer 2 Neighbor View maps, the icon for the Aggregator Interface is yellow:

When an Interface Up occurs for all of the 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 440 for more information.

Aggregator Interface Down (*NNMi Advanced*)

Link Aggregation[1] or **Split Link Aggregation**[2]: 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 **AggregatorDown** Conclusion.

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

Source Object Updates, continued

Tab	Description
Incident	Adds the **Aggregator Interface Down** incident. Incident Name: `AggregatorDown` The **Correlated Children** tab has an **Interface Down** incident for the member interfaces that have a Status of **Critical**. Incident Name: `InterfaceDown`
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

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 **Critical**.
Status	Adds the **Minor** Status.
Conclusions	**InterfacesDownInNode**

See "Interface Down" on page 512 for more information about Interface Down incidents.

On Layer 2 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 440 for more information.

Aggregator Connection Degraded (*NNMi Advanced*)

Link Aggregation[1] or **Split Link Aggregation**[2]: 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 492.

An Aggregator Connection 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 **AggregatorLinkDegraded** Conclusion.
Incident	Adds the **Aggregator Connection Degraded** incident. Incident Name: `AggregatorLinkDegraded` The **Correlated Children** tab has an **Aggregator Degraded** incident for each Aggregator Interface. Incident Name: `AggregatorDegraded`
Status	Adds the **Minor** Status.
Overall Status	Changes to **Minor**.

On the Source Node form, NNMi updates information on the following tabs:

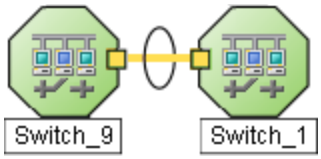
Source Node Updates

Tab	Description
Interfaces	Changes the State and Status of all Aggregation Member Interfaces that have an Operational State of Down to **Critical**.
Status	Adds the **Minor** Status.
Conclusions	**InterfacesDownInNode**

See "Interface Down" on page 512 for more information about Interface Down incidents.

On Layer 2 maps, the icon for the Aggregator Layer 2 Connection is yellow:

[1]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).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.



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 440 for more information.

Aggregator Connection Down (*NNMi Advanced*)

Link Aggregation[1] or **Split Link Aggregation**[2]: NNMi 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 (NNMi Advanced)" on page 493.

An Aggregator Connection 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 **AggregatorLinkDown** Conclusion.
Incident	Adds the **Aggregator Connection Down** incident. Incident Name: `AggregatorLinkDown` The **Correlated Children** tab includes the **Aggregator Down** incidents under this incident. Incident Name: `AggregatorDown`
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

On the Source Node form, NNMi updates information on the following tabs:

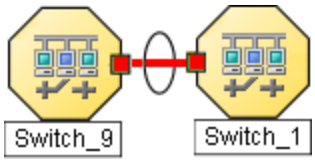
[1]Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface).
[2]Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

Source Node Updates

Tab	Description
Interfaces	Changes the State and Status of all member interfaces that have an Operational State of Down to **Critical**.
Status	Adds the **Minor** Status.
Conclusions	**InterfacesDownInNode**

See "Interface Down" on page 512 for more information about Interface Down incidents.

On Layer 2 maps, the icon for the Aggregator Connection is red:



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 440 for more information.

All Cards Down in Chassis

NNMi generates an **All Cards Down in Chassis** incident when all Cards in the Chassis have an **Operational State** of **Down**.

An **All Cards Down in Chassis** incident has Severity set to **Major**.

On the Source Object form NNMi updates information on the following tabs:

Source Object Updates

Tab	Description
Incident	Adds the **All Cards Down in Chassis** incident. Incident Name: `AllCardsDownInChassis` If a **Card Down** incident is generated within 5 minutes of an **All Cards in Chassis Down** incident, the **Correlated Children** tab includes the **Card Down** incidents. Incident Name: `CardDown` When all cards for the **Managed By** node are in this Chassis, NNMi generates only the **Node Down** incident.

Source Object Updates, continued

Tab	Description
	Incident Name: `NodeDown`
Status	Changes the Overall Status to **Major**. And adds the **Major** Status to the Status History.
Conclusion	Adds the **AllCardsDownInChassis** Conclusion.

On the Source Node form, NNMi updates information on the following tabs:

Source Node Updates

Tab	Description
Status	Adds the **Warning** Status. And adds the **Warning** Status to the Status History.
Conclusions	**ChassisDegradedIInNode**

See "Cards Down in Chassis" on page 504 and "Card Down" on page 501 for more information.

On the maps, the icon for the Source Node is set to teal:

When NNMi determines that all Cards in the Chassis have an Operational State of Up, NNMi updates the following attributes:

- The Chassis Status is changed to **Normal**.
- Each associated Card Status is changed to **Normal**.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 440 for more information.

See "Card Form" on page 211 and "Chassis Form" on page 193 for more information about Card and Chassis State and Status.

Backplane is Out of Configured Range

A **Backplane on <*NodeName*> is out of configured range** incident indicates the source Node has a backplane that is outside of the configured threshold range (too full, too empty).

A **Backplane on <*NodeName*> is out of configured 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
Physical Sensors (*only if Source Object is a Chassis or Card*)	The State and Status of the Physical Sensor that detected a malfunctioning backplane is changed to **Critical**.
Conclusion	Adds the **BackplaneOutOfRangeOrMalfunctioning** Conclusion.

Source Object Updates, continued

Tab	Description
Incident	Adds the **Backplane on <*NodeName*> is out of configured range** incident. Incident Name: `BackplaneOutOfRangeOrMalfunctioning` The **Correlated Children** tab includes any associated traps. See also "Backplane Incidents (NNM iSPI Performance for Metrics)" on page 548.
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

On the Source Node form, NNMi updates information on the following tabs:

Node Updates

Tab	Description
Physical Sensors	The State and Status of the Physical Sensor that detected a malfunctioning backplane is changed to **Critical**.
Chassis	The associated chassis' (if any) status changes to Major. • If the relevant sensor is hosted on a card in the chassis, the chassis' conclusion is **CardMajorInChassis**. • If the relevant sensor is hosted on the chassis, the chassis' conclusion is **ChassisWithBadBackplane**.
Card	If the relevant sensor is hosted on a card, the card status changes to Major with a conclusion of **CardWithBadBackplane**.
Status	The Node Status changes to **Major**. On the maps, the Source Node icon color changes to orange:
Conclusions	**ChassisMajorInNode**

When NNMi determines that the backplane is functioning properly, NNMi updates the following attributes:

- The Physical Sensor's Status changes to **Normal**.
- The Physical Sensor's Conclusion changes to `BackplaneInRangeAndFunctioning`.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 440 for more information.
- The associated Chassis's Status changes to **Normal** and the Conclusion `ChassisWithBadBackplane` or `CardMajorInChassis` is removed.
- If the sensor is hosted on a card, the Card's Status changes to **Normal** and the Conclusion `CardWithBadBackplane` is removed.
- On the Node form, the Node status changes to **Normal**. On the maps, the Source Node icon color changes to green:

See Also

"Backplane Incidents (NNM iSPI Performance for Metrics)" on page 548

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 **BufferOutOfRangeOrMalfunctioning** Conclusion.
Incident	Adds the **Buffer has Insufficient Capacity or is Malfunctioning** incident. Incident Name: `BufferOutOfRangeOrMalfunctioning` The **Correlated Children** tab includes any associated traps.
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

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 440 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 child cards.

On the Source Object form, NNMi updates information on the following tabs:

Source Object Updates

Tab	Description
Conclusion	Adds the **CardDisabled** Conclusion. **Note:** If the SNMP Agent reports the card has an Operational State of Down, then NNMi also adds a **CardDown** conclusion. The **Card Down** incident is not generated.
Incident	Adds the **Card Disabled** incident. Incident Name: `CardDisabled` The **Correlated Children** tab includes any associated traps.
Status	Adds the **Disabled** Status.
Overall Status	Changes to **Disabled**

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 440 for more information.

See "Card Form" on page 211 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 Child 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
Incident	Adds the **Card Down** incident. Incident Name: `CardDown` If you display the Incident's form, the **Correlated Children** tab includes the following: • All **ConnectionDown** and **InterfaceDown** incidents that are associated with this Card under this incident. • Any associated traps.

Source Object Updates, continued

Tab	Description
Status	Changes the Overall Status to **Critical**. And adds the **Critical** Status to the Status History.
Conclusions	Adds the **CardDown** Conclusion.

On the Parent Card's form (if any), NNMi updates information on the following tabs:

Parent Card Updates (if any)

Tab	Description
Status	Changes the Overall Status to **Minor**. And adds the **Minor** Status to the Status History.
Conclusions	Adds the **DaughterCardsDown** Conclusion.

On the Parent Chassis' form (if any), NNMi updates information on the following tabs:

Chassis Updates (if any)

Tab	Description
Incidents	No incident if only one card is down. "Cards Down in Chassis" on page 504 (if more than one card down in the chassis) Incident Name: `CardsDownInChassis` "All Cards Down in Chassis " on page 497 (if all cards down in the chassis) Incident Name: `AllCardsDownInChassis`
Status	Changes the Overall Status to **Warning**. Adds the **Warning** Status to the Status History.
Conclusions	Adds one of the following Conclusions, as appropriate: **ChassisDown** (all cards down) **CardDownInChassis**. **CardsDownInChassis** (more than one card down but not all) **AllCardsDownInChassis** (all cards down)

On the Source Node form, NNMi updates information on the following tabs:

Source Node Updates

Tab	Description
Cards	State and Status changes to **Critical** for any Cards with an Operational State of Down.
Interfaces	State and Status changes to **Critical** for any Interfaces with an Operational State of Down.
Status	Node without Chassis: Changes Overall Status to **Minor**. On the maps, the icon for the

Source Node Updates, continued

Tab	Description
	Source Node is set to yellow: Node with Chassis: Changes Overall Status to **Warning**. On the maps, the icon for the Source Node is set to teal:
Conclusions	Adds one of the following Conclusions, as appropriate if the Node has a Chassis: **ChassisWarningInNode** (one card down) **ChassisDegradedInNode** (more than one card down)

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:

- On the Card form:
  - The Card Status changes to **Normal**.
  - The Card Conclusion changes to **CardUp**.
- On the Chassis form (if any):
  - The Chassis Status changes to **Normal**.
  - The Chassis Conclusion changes to **ChassisUp**.
- On the Incident form's General tab:
  - The **Correlation Notes** text changes.
  - The Lifecycle State changes to **Closed**.
- On the Node form:
  - The Node Status changes to **Normal**. On the maps, the icon for the Source Node is set to green:

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 State 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
Incident	Adds the **Card Undetermined State** incident. Incident Name: `CardUndeterminedState`
Status	Changes the Overall Status to **Minor**. Adds the **Minor** Status to the Status History.
Conclusion	Adds the **CardUndeterminedState** Conclusion.

This incident does not affect the Source Node's Status.

When NNMi determines that the card has an Operational State of Up, NNMi updates the following attributes:

- On the Card form:
  - The Card Status changes to **Normal**.
  - The Card Conclusion changes to **CardUp**.
- On the Chassis form (if any):
  - The Chassis Status changes to **Normal**.
  - The Chassis Conclusion changes to **ChassisUp**.
- On the Incident form's General tab:
  - The **Correlation Notes** text changes.
  - The Lifecycle State changes to **Closed**.

See "Card Form" on page 211 for more information about card States and Status.

Cards Down in Chassis

You receive a **Cards Down in Chassis** incident when NNMi determines the following:

- Multiple Cards in the Chassis have an **Operational State** of **Down**.
- Not all Cards in the Chassis have an **Operational State** of **Down**.

A **Cards Down in Chassis** 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
Incident	Adds the **Cards Down in Chassis** incident. Incident Name: `CardsDownInChassis`

Source Object Updates, continued

Tab	Description
	The **Correlated Children** tab includes all **Card Down** incidents that are associated with this chassis within the last 5 minutes. Incident Name: `CardDown`
Status	Changes the Overall Status to **Minor**. And adds the **Minor** Status to the Status History.
Conclusion	Adds the **CardsDownInChassis** Conclusion.

On the Source Node form, NNMi updates information on the following tabs:

Source Node Updates

Tab	Description
Status	Adds the **Warning** Status. Changes Overall Status to **Warning**. On the maps, the icon for the Source Node is set to teal:
Conclusions	**ChassisDegradedInNode**

When NNMi determines that all Cards in the Chassis have an Operational State of Up, NNMi updates the following attributes:

- On the Card form:
  - The Card Status changes to **Normal**.
  - The Card Conclusion changes to **CardUp**.
- On the Chassis form:
  - The Chassis Status changes to **Normal**.
  - The Chassis Conclusion changes to **ChassisUp**.
- On the Incident form's General tab:
  - The **Correlation Notes** text changes.
  - The Lifecycle State changes to **Closed**.
- On the Node form:
  - The Node Status changes to **Normal**. On the maps, the icon for the Source Node is set to green:

Chassis Disabled

You receive a **Chassis Disabled** incident when an SNMP agent reports that a Chassis has an Administrative State of Down.

A **Chassis Disabled** 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 **ChassisDisabled** Conclusion.
Incident	Adds the **Chassis Disabled** incident. Incident Name: `ChassisDisabled`
Status	Adds the **Disabled** Status.
Overall Status	Changes to **Disabled**.

On the maps, the icon for the Source Node is set to yellow.

When NNMi determines that the Chassis is no longer Disabled, NNMi updates the following attributes:

- The Chassis Status changes to **Normal**.
- The Chassis Conclusion changes to **ChassisUp**.
- NNMi updates Information in the Correlation Notes attribute and closes the incident. See "Incident Form: General Tab" on page 440 for more information.

See "Chassis Form" on page 193 for more information about Chassis States and Status.

Chassis Down

You receive a **Chassis Down** incident when NNMi determines the Chassis has an **Operational State** of **Down**.

A **Chassis 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 **ChassisDown** Conclusion.
Incident	Adds the **Chassis Down** incident. Incident Name: `ChassisDown` If the **Chassis Down** incident is generated within 5 minutes of an **All Cards Down in Chassis** incident, the **Correlated Children** tab includes the **All Cards Down in Chassis** incident associated with the Chassis. Incident Name: `AllCardsDownInChassis` When all cards for the **Managed By** node are in this Chassis, NNMi generates only the **Node Down** incident.
Status	Adds the **Critical** Status.

Source Object Updates, continued

Tab	Description
Overall Status	Changes to **Critical**.

On the Source Node form, NNMi updates information on the following tabs:

Source Node Updates

Tab	Description
General	Changes the State Node on which the Chassis resides to **Minor**.
Status	Adds the **Minor** Status.
Conclusions	**ChassisDownInNode**

On the maps, the icon for the Source Node is set to yellow:

When NNMi determines that all Cards in each Chassis have an Operational State of Up and the Chassis State is no longer Down, NNMi updates the following attributes:

- The Chassis Status changes to **Normal**.
- The Chassis Conclusion changes to **ChassisUp**.
- NNMi updates Information in the Correlation Notes attribute and closes the incident. See "Incident Form: General Tab" on page 440 for more information.

See "Chassis Form" on page 193 for more information about Chassis States and Status.

Connection Down

NNMi periodically uses the management protocols available 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

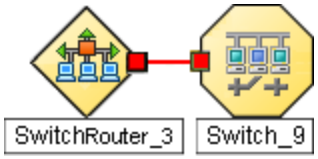
Tab	Description
Conclusion	Adds the **ConnectionDown** Conclusion.
Incident	Adds the **Connection Down** incident. Incident Name: `ConnectionDown`
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

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 **Critical**.
Status	Adds the **Minor** Status.
Conclusions	**InterfacesDownInNode**

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 440 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 **CpuOutOfRangeOrMalfunctioning** Conclusion.
Incident	Adds the **CPU Utilization is too High** incident.

Source Object Updates, continued

Tab	Description
	Incident Name: `CpuOutOfRangeOrMalfunctioning` The **Correlated Children** tab includes any associated traps.
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

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 440 for more information.

Custom Polled Instance in Collection is Out of Range

Note: The NNMi administrator determines whether NNMi generates **Custom Polled Instance**[1] 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**[2].

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 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 Node's short DNS Name followed by the MIB Instance value in the format: <*node_name*> -<*MIB_instance_value*>. This value also appears in Line Graphs and as the Display Attribute in the Custom Polled Instance View. If you are an NNMi administrator, see MIB Expressions Form (Custom Poller) for more information.

[1]A Custom Polled Instance represents the results of a MIB variable when it is evaluated against a node. The first time a MIB variable 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.
[2]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.

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 **Custom Polled Instance in Collection is Out of Range** incident. Incident Name: `CustomPolledInstanceOutOfRange`
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 440 for more information.

Fan is Out of Range or Malfunctioning

A **Fan is Out of Range or Malfunctioning** incident indicates the source Node has a fan that is not operating correctly.

A **Fan is Out of Range or 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
Physical Sensors (*only if Source Object is a Chassis or Card*)	The State and Status of the Physical Sensor that detected a malfunctioning fan is changed to **Critical**.
Conclusion	Adds the **FanOutOfRangeOrMalfunctioning** Conclusion.
Incident	Adds the **Fan is Out of Range or Malfunctioning** incident.

Source Object Updates, continued

Tab	Description
	Incident Name: `FanOutOfRangeOrMalfunctioning` The **Correlated Children** tab includes any associated traps.
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

On the Source Node form, NNMi updates information on the following tabs:

Node Updates

Tab	Description
Physical Sensors	The State and Status of the Physical Sensor that detected a malfunctioning fan is changed to **Critical**.
Chassis	The associated chassis' (if any) status changes to Major. • If the relevant sensor is hosted on a card in the chassis, the chassis' conclusion is **CardMajorInChassis**. • If the relevant sensor is hosted on the chassis, the chassis' conclusion is **ChassisWithBadFan**.
Card	If the relevant sensor is hosted on a card, the card status changes to Major with a conclusion of **CardWithBadFan**.
Status	The Node Status changes to **Major**. On the maps, the Source Node icon color changes to orange:
Conclusions	**ChassisMajorInNode**

When NNMi determines that the fan is functioning properly, NNMi updates the following attributes:

- The Physical Sensor's Status changes to **Normal**.
- The Physical Sensor's Conclusion changes to `FanInRangeAndFunctioning`.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 440 for more information.
- The associated Chassis's Status changes to **Normal** and the Conclusion `ChassisWithBadFan` or `CardMajorInChassis` is removed.
- If the sensor is hosted on a card, the Card's Status changes to **Normal** and the Conclusion `CardWithBadFan` is removed.
- On the Node form, the Node status changes to **Normal**. On the maps, the Source Node icon color changes to green:

Interface Down

NNMi periodically uses the management protocols available to check each interface. For example, 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 **InterfaceDown** Conclusion.
Incident	Adds the **Interface Down** incident which means MIB-II ifOperStatus= down. Incident Name: `InterfaceDown` The **Correlated Children** tab includes any associated link down traps. **Tip:** If MIB-II ifAdminStatus = administratively down, NNMi can generate the "Interface Disabled" on the next page instead of this Interface Down incident.
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

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 **Critical**. **Note:** You might find relevant traps on the **Correlated Children** tab.
Addresses	If the interface has one or more addresses, the State and Status is **Critical** if the address is no longer reachable.
Status	Adds the **Minor** Status.
Conclusions	**InterfacesDownInNode**

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 440 for more information.
- The Node Status is changed to **Normal**. The Conclusion on the Node is `InterfaceUpInNode`.

Interface Disabled

NNMi periodically uses the management protocols available to check each interface. For example, 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 **InterfaceDisabled** Conclusion.
Incident	Adds the **Interface Disabled** incident which means MIB-II ifAdminStatus = administratively down. Incident Name: `InterfaceDisabled` The **Correlated Children** tab includes any associated link down traps. **Tip:** If MIB-II ifOperStatus = down, NNMi can generate the "Interface Down" on the previous page instead of this Interface Disabled incident.
Status	Adds the **Disabled** Status. (NNMi Advanced). If a management protocol indicates that the Power State of a virtual machine is **Powered Off** or **Suspended**, the Interface Status of all uplinks is Disabled.

Source Object Updates, continued

Tab	Description
Overall Status	Changes to **Disabled**.
Associated IP Addresses	Adds the `AddressDisabled` 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 440 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**.

Incident Name: `IpSubnetContainsIpWithNewMac`

NNMi cannot determine the Source Node, so this incident only appears in Incident views (never on a source object's Incidents tab).

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 **MemoryOutOfRangeOrMalfunctioning** Conclusion.
Incident	Adds the **Memory has Insufficient Capacity or is Malfunctioning** incident. Incident Name: `MemoryOutOfRangeOrMalfunctioning` The **Correlated Children** tab includes any associated traps.
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

On the Source Node form, NNMi updates information on the following tabs:

Source Node Updates

Tab	Description
Node Sensors	Changes the State and Status of the malfunctioning memory to **Critical.**
Status	Adds the **Major** Status.
Conclusions	**NodeWithBadMemory**

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 440 for more information.
- The Source Node Conclusion is changed to NodeWithGoodMemory.

Node or Connection Down

If a node is not responding to ICMP or other available management protocols, 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:

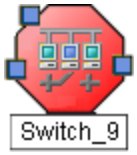
Source Object Updates

Tab	Description
Conclusion	Adds the **NodeOrConnectionDown** Conclusion.
Incident	Adds the **Node or Connection Down** incident. Incident Name: `NodeOrConnectionDown` On the **Correlated Children** tab, any **Interface Down** incident on neighbors that are one hop from the node are correlated under this **Node or Connection Down** incident.
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

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 519 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 440 for more information.

Node Paused (NNMi Advanced)

NNMi periodically uses the management protocols available to check each device. If a management protocol indicates that the device is suspended or paused, NNMi generates a Node Paused incident.

A **Node Paused** incident is generated with Severity set to **Disabled**.

On the Source Object form, NNMi updates information on the following tabs:

Source Object Updates

Tab	Description
Conclusion	Adds the **Node Paused** Conclusion.
Incident	Adds the **Node Paused** incident.
Status	Adds the **Disabled** Status.
Overall Status	Changes to **Disabled**.
Associated IP Addresses	Changes the Status to **Not Responding**.
Associated Interfaces	Changes the Status to **Disabled**.

Map Displays

The Status of the device for a Source Node changes to **Disabled** and the device's map icon color changes to gray. The status of each interface changes to **Disabled** and the interface map icon color changes to gray.

When NNMi determines that the Node is Up, NNMi updates the following attributes:

- The Node 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 440 for more information.

Node Powered Down (NNMi Advanced)

NNMi periodically uses the management protocols available to check each device. If a management protocol indicates that the device is turned off, NNMi generates a **Node Powered Down** incident.

A **Node Powered Down** incident is generated with Severity set to **Disabled**.

On the Source Object form, NNMi updates information on the following tabs:

Source Object Updates

Tab	Description
Conclusion	Adds the **NodePoweredDown** Conclusion.
Incident	Adds the **Node Powered Down** incident .

Source Object Updates, continued

Tab	Description
Status	Adds the **Disabled** Status.
Overall Status	Changes to **Disabled**.
Associated IP Addresses	Changes the Status to **Not Responding**.
Associated Interfaces	Changes the Status to **Disabled**.

Map Displays

The Status of the device for a Source Node changes to **Disabled** and the device's map icon color changes to gray. The status of each interface changes to **Disabled** and the interface map icon color changes to gray.

When NNMi determines that the Node is Up, NNMi updates the following attributes:

- The Node 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 440 for more information.

Power Supply is Out of Range or Malfunctioning

A **Power Supply is Malfunctioning** incident indicates the source Node has a power supply that is not operating correctly.

A **Power Supply 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 **PowerSupplyOutOfRangeOrMalfunctioning** Conclusion.
Incident	Adds the **Power Supply is Malfunctioning** incident. Incident Name: `PowerSupplyOutOfRangeOrMalfunctioning` The **Correlated Children** tab includes any associated traps.
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

On the Source Node form, NNMi updates information on the following tabs:

Node Updates

Tab	Description
Physical Sensors	The State and Status of the Physical Sensor that detected a malfunctioning power supply is changed to **Critical**.
Chassis	The associated chassis' (if any) status changes to Major. • If the relevant sensor is hosted on a card in the chassis, the chassis' conclusion is **CardMajorInChassis**. • If the relevant sensor is hosted on the chassis, the chassis' conclusion is **ChassisWithBadPowerSupply**.
Card	If the relevant sensor is hosted on a card, the card status changes to Major with a conclusion of **CardWithBadPowerSupply**.
Status	The Node Status changes to **Major**. On the maps, the Source Node icon color changes to orange:
Conclusions	**ChassisMajorInNode**

When NNMi determines that the power supply is functioning properly, NNMi updates the following attributes:

- The Physical Sensor's Status changes to **Normal**.
- The Physical Sensor's Conclusion changes to `PowerSupplyInRangeAndFunctioning`.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 440 for more information.
- The associated Chassis's Status changes to **Normal** and the Conclusion `ChassisWithBadPowerSupply` or `CardMajorInChassis` is removed.
- If the sensor is hosted on a card, the source Card's Status changes to **Normal** and the Conclusion `CardWithBadPowerSupply` is removed.
- On the Node form, the Node status changes to **Normal**. On the maps, the Source Node icon color changes to green:

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.

- (NNMi Advanced.) A virtual machine has at least one virtual switch that is disabled.
- (NNMi Advanced). The virtual machine guest operating system has failed.

A Node Down incident is generated with Severity set to **Critical**, and the map icon is set to red (see Map Displays).

Tip: (*Optional NNM iSPI Performance for Metrics*) If this incident represents planned maintenance and not an unexpected outage, to update the end-of-month report:

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

1. Right-click the incident and select **Node Actions** → **Management Mode** → **Schedule Node Outage**.
2. Configure the details, see "Scheduling Outages for Nodes or Node Groups" on page 322. By default, NNMi proves a Start Time five minutes prior to the Incident's start time.
3. Click **Record a Past Outage**.

On the Source Object form, NNMi updates information on the following tabs:

Source Object Updates

Tab	Description
Conclusion	Adds the **NodeDown** Conclusion.
Incident	Adds the **Node Down** incident. Incident Name: `NodeDown` On the **Correlated Children** tab, any **Interface Down** incident on neighbors that are one hop from the node are correlated under this **Node Down** incident.
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

Note: When NNMi cannot determine whether the node or connection is down, it generates a **Node or Connection Down** incident. See "Node or Connection Down" on page 515 for more information.

NNMi does not generate a Node Down incident for node under the following conditions:

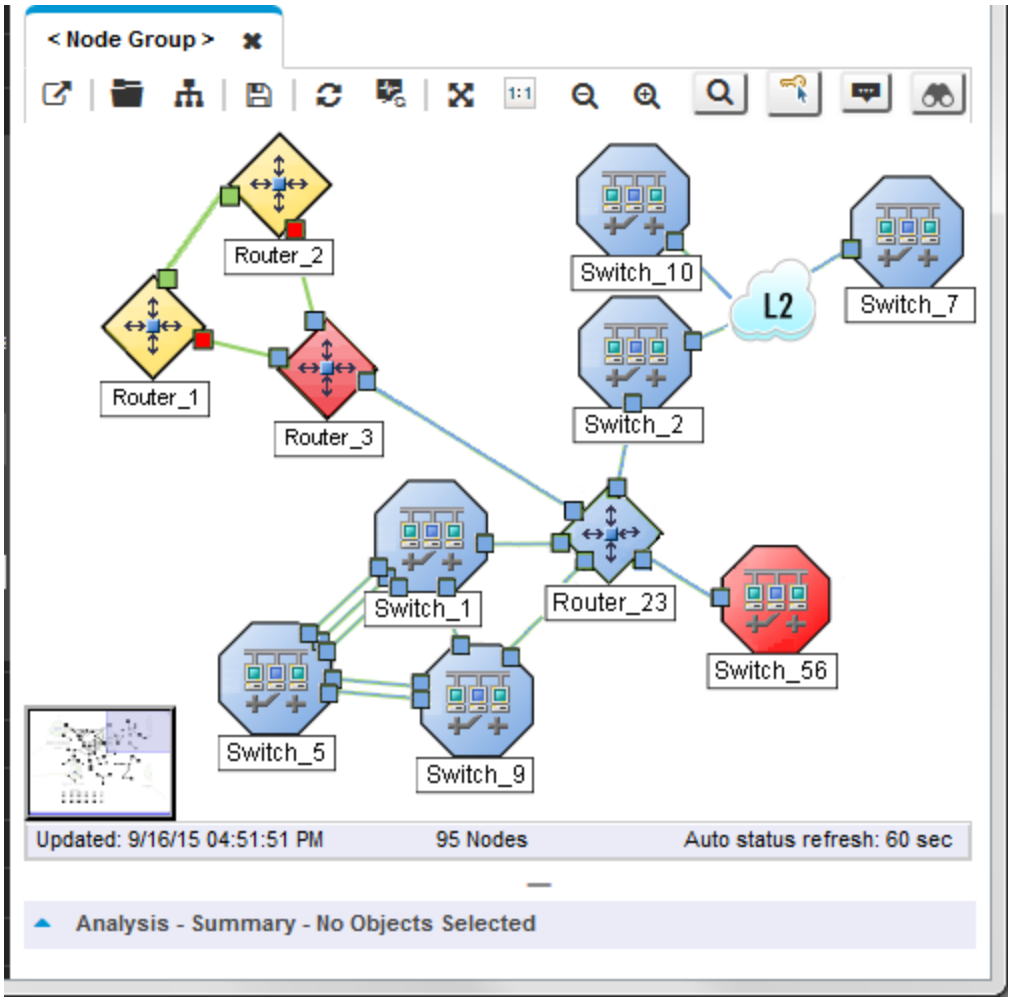
- If the node is in the shadow of another node that causes the node to be unreachable.
- If the node is in an ATM or Frame Relay cloud that causes the node to be unreachable.

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 440 for more information.

Remote Site Unreachable

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.NNMi checks for Islands and, when applicable, automatically creates them whenever it detects changes in Layer 2 Connections.

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.

A **Remote site containing node <X> is unreachable** incident is generated when all of the nodes within an Island do not respond to both ICMP and SNMP queries.

X = NNMi selects a representative node in the Island Group as the Source Node associated with this incident. On the Source Node's form, NNMi provides the following:

Source Node Updates

Tab	Description
Incident	Adds the **Remote site containing node <X> is unreachable** incident. Incident Name: `IslandGroupDown` When NNMi determines that a node in the Island Group responds to either ICMP or SNMP queries, NNMi updates the information in this incident's **Correlation Notes** attribute and closes this incident. See "Incident Form: General Tab" on page 440 for more information.

Stack Degraded (*NNMi Advanced*)

You receive a **Stack Degraded** incident when NNMi analyzed the situation and determined the following:

- One Chassis has a MASTER State
- One Chassis has a SLAVE State
- Other Chassis in the group are not in SLAVE State

A **Stack Degraded** incident is generated with Severity set to **Minor**.

Note: All of the managed objects (Cards, Interfaces, Physical Sensors) contained in the Chassis are set to a Status of Unknown.

On the Source Object form, NNMi updates information on the following tabs:

Source Object Updates

Tab	Description
Incident	Adds the **Stack Degraded** incident. Incident Name: `StackDegraded` If you display the Incident's form, the **Correlated Children** tab includes the following: • All **Chassis Down**, **Aggregator Connection Down** and **Aggregator Connection Degraded** incidents that are associated with a Chassis in the Chassis Redundancy Group. • Any associated traps.
Status	Changes Overall Status to **Minor**. Adds the **Minor** Status to the Status History.
Conclusions	Adds the **StackDegraded** Conclusion.

On the Source Node's form, NNMi provides the following:

Source Node Updates

Tab	Description
Status	Changes Overall Status to **Warning**.
Conclusions	Adds the StackDegradedInNode Conclusion.

Stack with no Slave (*NNMi Advanced*)

You receive a **Stack With No Slave** incident when NNMi analyzed the situation and determined that no Chassis in the Chassis Redundancy Group has a standby State value of SLAVE.

A **Stack With No Slave** incident is generated with Severity set to **Major**.

Note: All of the managed objects (Cards, Interfaces, Physical Sensors) contained in the Chassis are set to a Status of Unknown.

On the Source Object form, NNMi updates information on the following tabs:

Source Object Updates

Tab	Description
Incident	Adds the **Stack with no Slave** incident. Incident Name: `StackWithNoSlave` If you display the Incident's form, the **Correlated Children** tab includes the following: • All **Chassis Down**, **Aggregator Connection Down** and **Aggregator Connection**

Source Object Updates, continued

Tab	Description
	Degraded incidents that are associated with a Chassis in the Chassis Redundancy Group. • Any associated traps.
Status	Changes Overall Status to **Major**. Adds the **Major** Status to the Status History.
Conclusions	Adds the **StackWithNoSlave** Conclusion.

On the Source Node's form, NNMi provides the following:

Source Node Updates

Tab	Description
Status	Changes Overall Status to **Minor**.
Conclusions	Adds the StackMinorInNode Conclusion.

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:

SNMP Agent (Source Object) Form Updates

Tab	Description
Conclusion	Adds the **SNMPAgentNotResponding** Conclusion.
Incident	Adds the **SNMP Agent Not Responding** incident. Incident Name: `SNMPAgentNotResponding`
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

On the Source Node form, NNMi updates information on the following tabs:

Source Node Form Updates When SNMP Agent Is Down

Tab	Description
Cards	The Status of polled Cards is set to **Unknown**.
Chassis	The Status of the Chassis is set to **Unknown**.
Interfaces	The Status of polled Interfaces is set to **Unknown**.
Status	Adds the **Minor** Status.
Conclusions	**UnresponsiveAgentInNode**

Card Form Updates When SNMP Agent Is Down

Tab	Description
Status	Adds the **Unknown** Status.
Conclusions	**CardUnmanageable**

Chassis Form Updates When SNMP Agent Is Down

Tab	Description
Status	Adds the **Unknown** Status.
Conclusions	**ChassisUnmanageable**

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 440 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 440 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.
- The Node's Chassis returns to its previous Status and the **ChassisUnmanageable** Conclusion is cleared.

Temperature Sensor is Out of Range

A **Temperature Sensor is Out of Range** incident indicates source Node's temperature 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
Physical Sensors (*only if Source Object is a Chassis or Card*)	The State and Status of the Physical Sensor that detected a malfunctioning temperature is changed to **Critical**.
Conclusion	Adds the **TemperatureOutOfRangeOrMalfunctioning** Conclusion.
Incident	Adds the **Temperature Sensor is Out of Range** incident. Incident Name: `TemperatureOutOfRangeOrMalfunctioning` The **Correlated Children** tab includes any associated traps.
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

On the Source Node form, NNMi updates information on the following tabs:

Node Updates

Tab	Description
Physical Sensors	The State and Status of the Physical Sensor that detected an out-of-range Temperature is changed to **Critical**.
Chassis	The associated chassis' (if any) status changes to Major. • If the relevant sensor is hosted on a card in the chassis, the chassis' conclusion is **CardMajorInChassis**. • If the relevant sensor is hosted on the chassis, the chassis' conclusion is **ChassisWithBadTemperature**.
Card	If the relevant sensor is hosted on a card, the card status changes to Major with a conclusion of **CardWithBadTemperature**.
Status	The Node Status changes to **Major**. On the maps, the Source Node icon color changes to orange:
Conclusions	**ChassisMajorInNode**

When NNMi determines that the Temperature is functioning properly, NNMi updates the following attributes:

- The Physical Sensor's Status changes to **Normal**.
- The Physical Sensor's Conclusion changes to `TemporatureInRangeAndFunctioning`.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 440 for more information.
- The associated Chassis's Status changes to **Normal** and the Conclusion `ChassisWithBadTemperature` or `CardMajorInChassis` is removed.
- If the sensor is hosted on a card, the Card's Status changes to **Normal** and the Conclusion `CardWithBadTemperature` is removed.
- On the Node form, the Node status changes to **Normal**. On the maps, the Source Node icon color changes to green:

Voltage is Out of Range

A **Voltage is Out of Range** incident indicates the source Node's power supply voltage 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
Physical Sensors (*only if Source Object is a Chassis or Card*)	The State and Status of the Physical Sensor that detected a malfunctioning voltage regulator is changed to **Critical**.
Conclusion	Adds the **VoltageOutOfRangeOrMalfunctioning** Conclusion.
Incident	Adds the **Voltage is Out of Range** incident. Incident Name: `VoltageOutOfRangeOrMalfunctioning` The **Correlated Children** tab includes any associated traps.
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**

On the source Node form, NNMi updates information on the following tabs:

Node Updates

Tab	Description
Physical Sensors	The State and Status of the Physical Sensor that detected a problem with the power supply voltage is changed to **Critical**.
Chassis	The associated chassis' (if any) status changes to Major. • If the relevant sensor is hosted on a card in the chassis, the chassis' conclusion is **CardMajorInChassis**.

Node Updates, continued

Tab	Description
	• If the relevant sensor is hosted on the chassis, the chassis' conclusion is **ChassisWithBadVoltage**.
Card	If the relevant sensor is hosted on a card, the card status changes to Major with a conclusion of **CardWithBadVoltage**.
Status	The Node Status changes to **Major**. On the maps, the Source Node icon color changes to orange:
Conclusions	**ChassisMajorInNode**

When NNMi determines that the Voltage is functioning properly, NNMi updates the following attributes:

- The Physical Sensor's Status changes to **Normal**.
- The Physical Sensor's Conclusion changes to `VoltageInRangeAndFunctioning`.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 440 for more information.
- The associated Chassis's Status changes to **Normal** and the Conclusion `ChassisWithBadVoltage` or `CardMajorInChassis` is removed.
- If the sensor is hosted on a card, the Card's Status changes to **Normal** and the Conclusion `CardWithBadVoltage` is removed.
- On the Node form, the Node status changes to **Normal**. On the maps, the Source Node icon color changes to green:

Web Agent Not Responding (NNMi Advanced)

NNMi periodically checks the availability of each **Web Agent**[1] in your network environment. Possible reasons a Web Agent is not responding include the following:

- The device credentials for the Web Agent are no longer valid and need to be updated.
- There is an issue with the hypervisor hosting the Web Agent, and the agent is no longer responding to requests for state information from NNMi.
- The hypervisor hosting the Web Agent is currently not reachable from the NNMi management server.

A **Web Agent Not Responding** incident is generated with Severity set to **Minor**.

On the Source Object form, NNMi updates information on the following tabs:

Web Agent (Source Object) Form Updates

Tab	Description
Conclusion	Adds the **WebAgentNotResponding** Conclusion.
Incident	Adds the **Web Agent Not Responding** incident.

[1]The Web Agent represents a management service running on a device and contains the settings NNMi uses to communicate with the device.

Web Agent (Source Object) Form Updates, continued

Tab	Description
	Incident Name: `WebAgentNotResponding`
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

On the Source Node form, NNMi updates information on the following tabs:

Source Node Form Updates When Web Agent Is Down

Tab	Description
Interfaces	The Status of polled Interfaces is set to **Unknown**.
Status	Adds the **Minor** Status.
Conclusions	**UnresponsiveWebAgentInNode**

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 440 for more information.

When NNMi determines that Web Agent for the Source Node is responding, NNMi updates the following attributes:

- The Web Agent Status is changed to **Normal**.
- The Web Agent Conclusion is changed to **WebAgentResponding**.
- NNMi updates Information in the **Correlation Notes** attribute and closes the incident. See "Incident Form: General Tab" on page 440 for more information.
- The Node Status is changed to **Normal**. The Conclusion on the Node is **ResponsiveWebAgentInNode**.
- The Node's Interfaces return to their previous Status and the **InterfaceUnmanageable** Conclusion is cleared from the Node's polled Interfaces.

Interpret Incidents Related to SNMP Traps

Tip: Also see "Investigate and Diagnose Problems" on page 480 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" below
- "Pipeline Queue Size Exceeded Limit" on page 533
- "SNMP Trap Limit (Warning, Major or Critical)" on page 533
- "Trap Storm" on page 534

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 the next page
- "Message Queue Size Exceeded (NNMi Advanced)" on page 532

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	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. Note the following: • The report tracks the average trap rate over time. **Tip:** 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. • If the report exceeds the 2000 character limit, NNMi continues to log the information

Trap Information Source, continued

CIA	Description
	using subsequent files numbered consecutively; for example: `suppressedHosteObjects.1`, `suppressedHostedObjects.2`, and so on.
Unsuppressed Hosted Objects	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. Note the following: • The report tracks the average trap rate over time. **Tip:** 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. • If the report exceeds the 2000 character limit, NNMi continues to log the information using subsequent CIAs numbered consecutively; for example: `unsuppressedHosteObjects.1`, `unsuppressedHostedObjects.2`, and so on.

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.

When the trap rate returns to below the configured threshold, NNMi cancels the incident. See "Incident Form: General Tab" on page 440 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 29 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.

Note: The NNMi administrator must specifically configure SNMP Trap Incidents 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 29 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 **GlobalNetworkManagementIncidentQueueSizeLimitExceeded** 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 **GlobalNetworkManagementIncidentQueueSizeLimitExceeded** health conclusion with the Severity set to **Major**.
- Stops forwarding to Global Managers any incidents generated from SNMP Traps.

Note: The NNMi administrator must specifically configure SNMP Trap Incidents 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 Limit

A **Pipeline Queue Size Exceeded Limit** 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 Limit** 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 Limit** 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, 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 Incident 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 HPE 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 **SnmpTrapLimitExceeded** 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 **SnmpTrapLimitExceeded** 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 **SnmpTrapLimitExceeded** 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 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.
blocked Sources	The IP address for the Node, if any, that has suppressed traps. **Note:** This CIA vaue is `all` 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. **Note:** This CIA vaue is `all` if the overall trap rate is exceeded or if the overall trap rate for a specific node is exceeded.

When the trap rate returns to below the configured threshold, NNMi cancels the incident. See "Incident Form: General Tab" on page 440 for more information.

Interpret Informational Incidents

Tip: Also see "Investigate and Diagnose Problems" on page 480 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" on the next page

Card Removed

Tip:

- Also see "Investigate and Diagnose Problems" on page 480 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 **Card Removed** incident. The Correlated Children tab includes any associated traps.

Note: NNMi does not automatically close **Card Removed** incidents.

See "Card Form" on page 211 for more information about card States and Status.

Card Inserted

Tip: Also see "Investigate and Diagnose Problems" on page 480 for more information about troubleshooting tools that NNMi provides.

Tip: A **Card Inserted** incident indicates a Card has been inserted into the Source Node.

Tip: A **Card Inserted** Incident is generated with the Severity set to **Normal**.

Tip: On the Source Object (which is a node) form, NNMi updates information on the following tab:

Source Node Updates

Tab	Description
Incident	Adds the **Card Inserted** 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 480 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

The **Service Impact Incidents** view in the Incident Browsing workspace 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 affected 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.

The Service Impact incident helps your troubleshooting efforts by identifying which service is affected.

Note: NNMi's Causal Engine determines the Correlation Nature for an incident.

(*NNMi Advanced*) As an example of a Service Impact incident and its relationship with other incidents: an Interface Down incident on an interface that is part of a Router Redundancy Group can affect 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 539
- "Multiple Secondary Devices in Router Redundancy Group (NNMi Advanced)" on page 539
- "No Primary Card in Card Redundancy Group" on page 540
- "No Primary Device in Router Redundancy Group (NNMi Advanced)" on page 541
- "No Secondary Card in Card Redundancy Group" on page 542
- "No Secondary Device in Router Redundancy Group (NNMi Advanced)" on page 543
- "Primary Device in Router Redundancy Group Switched (NNMi Advanced)" on page 543
- "Router Redundancy Group Degraded (NNMi Advanced)" on page 544

Note: NNMi determines the Correlation Nature for an incident.

See "Router Redundancy Group View" on page 402 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 **CrgMultiplePrimary** Conclusion.
Incident	Adds the **Multiple Primary Cards in Card Redundancy Group** incident. The **Correlated Children** tab includes any associated traps. **Note:** If any cards in the group have an Operational State of Down, the **Card Down** incidents are correlated under the new incident
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

On the Source Node form, NNMi updates information on the following tabs:

Source Node Updates

Tab	Description
Status	Adds the **Warning** Status.
Conclusions	**CrgMalfunctionInNode**

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 440 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 **RrgMultiplePrimary** Conclusion.
Incident	Adds the **Multiple Primary Devices in Router Redundancy Group** incident. The **Correlated Children** tab includes any associated traps.
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

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 440 for more information.

When NNMi determines that the group has one primary member, NNMi udpates 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 440 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 **RrgMultipleSecondary** Conclusion.
Incident	Adds the **Multiple Secondary Devices in Router Redundancy Group** incident. The **Correlated Children** tab includes any associated traps.
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

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 **CrgNoPrimary** Conclusion.
Incident	Adds the **No Primary Card in Card Redundancy Group** incident. The **Correlated Children** tab includes any associated traps **Note:** If there are cards down in the group, the **Card Down** incidents is correlated under the new incident
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

On the Source Node form, NNMi updates information on the following tabs:

Source Node Updates

Tab	Description
Status	Adds the **Warning** Status.
Conclusions	**CrgMalfunctionInNode**

On the maps, the icon for the Source Node is set to teal.

When NNMi determines that the group contains a primary card, NNMi udpates 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 440 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 **RrgNoPrimary** Conclusion.
Incident	Adds the **No Primary Device in Router Redundancy Group** incident. The **Correlated Children** tab includes any associated traps. **Note:** If an interface in the group has an Operational State of Down, its **Interface Down** incident is correlated under this incident.
Status	Adds the **Critical** Status.
Overall Status	Changes to **Critical**.

When NNMi determines that the group has a Primary member, NNMi udpates 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 440 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 **CrgNoSecondary** Conclusion.
Incident	Adds the **No Secondary Card in Card Redundancy Group** incident. The **Correlated Children** tab includes any associated traps **Note:** If there are cards down in the group, the **Card Down** incidents are correlated under the new incident.
Status	Adds the **Minor** Status.
Overall Status	Changes to **Minor**.

On the Source Node form, NNMi updates information on the following tabs:

Source Node Updates

Tab	Description
Status	Adds the **Warning** Status.
Conclusions	**CrgMalfunctionInNode**

On the maps, the icon for the Source Node is set to teal.

When NNMi determines that the group contains a secondary card, NNMi udpates 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 440 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 **RrgNoSecondary** Conclusion.
Incident	Adds the **No Secondary Device in Router Redundancy Group** incident. The **Correlated Children** tab includes any associated traps. **Note:** If an interface in the group has an Operational State of Down, its **Interface Down** incident is correlated under this incident.
Status	Adds the **Warning** Status.
Overall Status	Changes to **Warning**.

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 **Primary Device in Router Redundancy Group Switched** incident. The **Correlated Children** 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 **Router Redundancy Group Degraded** incident. The **Correlated Children** tab includes any associated traps. **Note:** If an interface in the group has an Operational State of Down, the **Interface Down** incidents are correlated under this incident.
Status	Adds the **Warning** Status.
Overall Status	Changes to **Warning**.

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 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 Node form, Basic Attributes section for the currently configured address.	See "Management Address ICMP Response Time Incidents " on page 565

(*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
Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.	
Backplane Utilization Threshold based on the percentage of backplane usage compared to the total amount of available backplane resources.	See "Backplane Incidents (NNM iSPI Performance for Metrics)" on page 548
Buffer monitoring: • 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.	See "Buffer Incidents (NNM iSPI Performance for Metrics)" on page 550

Performance Threshold Incidents (NNM iSPI Performance for Metrics), continued

Threshold Being Monitored	Incidents
• 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 monitoring: • 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.	See "CPU Incidents (NNM iSPI Performance for Metrics)" on page 552
Disk Space Utilization Threshold based on the percentage of a node's disk space usage compared to the total amount of available disk space.	See "Disk Incidents (NNM iSPI Performance for Metrics)" on page 554
Interface Frame Check Sequence (FCS) monitoring: • FCS LAN Error Rate *Local Area Network interfaces only*.Threshold based on the percentage of incoming frames with a bad checksum (**CRC**[1] value) compared to the total number of incoming frames. Possible causes include collisions at half-duplex, a duplex mismatch, bad hardware (**NIC**[2], 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**[3] value) compared to the total number of incoming frames. Possible causes include wireless communication interference, bad hardware (**NIC**[4], cable or port), or a connected device generating frames with	See "Interface Frame Check Sequence (FCS) Error Rate Incidents (NNM iSPI Performance for Metrics)" on page 556

[1]Cyclic Redundancy Check
[2]Network Interface Controller
[3]Cyclic Redundancy Check
[4]Network Interface Controller

Performance Threshold Incidents (NNM iSPI Performance for Metrics), continued

Threshold Being Monitored	Incidents
bad Frame Check Sequence.	
Interface Discard Rate monitoring: • 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. • 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.	See "Interface Input and Output Discard Rate Incidents (NNM iSPI Performance for Metrics)" on page 557.
Interface Error Rate monitoring: • 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. • 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 as collisions and buffer errors.	See "Interface Input and Output Error Rate Incidents (NNM iSPI Performance for Metrics)" on page 559.
Interface Queue monitoring: • 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. • 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.	See "Input and Output Queue Drop Incidents (NNM iSPI Performance for Metrics)" on page 560.
Interface Utilization monitoring: • Input Utilization	See "Interface Input and Output Utilization Incidents (NNM iSPI Performance for Metrics)" on page

Performance Threshold Incidents (NNM iSPI Performance for Metrics), continued

Threshold Being Monitored	Incidents
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 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.	562.
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 567

Backplane Incidents (*NNM iSPI Performance for Metrics*)

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance

for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

Backplane incidents are available if the HPE Network Node Manager iSPI Performance for Metrics Software is installed and your NNMi administrator configured performance measurement thresholds. For more information:

Backplane incidents identify nodes that are over-used or under-used.

You receive backplane incidents when performance is not within the allowable range set by your NNMi administrator in Monitoring Configuration. 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 following tables describes the possible results.

Backplane Baseline Incidents

Baseline State Value	Incident	Incident Description	Incident Severity
Abnormal Range	Memory on <*NodeName*> is abnormal. Incident Name: `BackplaneAbnormal`	Physical Sensor measured an abnormal value according to Baseline Limits set by your NNMi administrator. This occurs when any backplane related metric is abnormal.	Warning
Normal	No incident is generated	The measured value is within the allowable range. NNMi closes any related Abnormal Range incidents.	Normal

Backplane Threshold Incidents

Threshold State Value	Incident	Incident Description	Incident Severity
Low None	Backplane on <*NodeName*> is out of configured range. Incident Name: `BackplaneOutOfRangeOrMalfunctioning`	Physical Sensor measured a value less than the allowable range according to the Threshold configured by your NNMi administrator and applied to members of a Node Group. See also "Backplane is Out of Configured Range" on page 498	Minor
Nominal	No incident is generated, and current incident changes to Lifecycle	The measured value is within the allowable range. NNMi closes any	Not applicable

Backplane Threshold Incidents, continued

Threshold State Value	Incident	Incident Description	Incident Severity
	State: Closed.	related High, Low, or None incidents.	
High	Backplane on <*NodeName*> is out of configured range. Incident Name: `BackplaneOutOfRangeOrMalfunctioning`	Physical Sensor measured a value more than the allowable range according to the Threshold configured by your NNMi administrator and applied to members of a Node Group.	Critical

When backplane Threshold State changes, NNMi updates to the information on the following Incident form tabs:

- Correlated Parents
- Correlated Children
- Custom Attributes

When NNMi determines that the Physical Sensor measurement is within the allowable range, NNMi updates the following attributes:

- The Physical Sensor Status is changed to **Normal**
- The Physical Sensor Conclusion is changed to one of the following:

Backplane Incident's Close Sequence

Physical Sensor Conclusion Initiating the Incident	Physical Sensor Conclusion Closing the Incident	Physical Sensor Status Changes To:
BackplaneAbnormal	BackplaneNormal	Normal
BackplaneOutOfRangeOrMalfunctioning	BackplaneInRangeAndFunctioning	Normal

This Physical Sensor Conclusion propagates to the following:

- "Card Form: Conclusions Tab" on page 226
- "Chassis Form: Conclusions Tab" on page 208
- "Node Form: Conclusions Tab" on page 95

Buffer Incidents (*NNM iSPI Performance for Metrics*)

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

Buffer incidents are available if the HPE Network Node Manager iSPI Performance for Metrics Software is installed and your NNMi 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 NNMi administrator in Monitoring Configuration. 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 following tables describe the possible results.

Buffer Baseline Incidents

Baseline State Value	Incident	Incident Description	Incident Severity
Abnormal Range	Buffer on <*NodeName*> is abnormal. Incident Name: `BufferAbnormal`	Node Sensor measured an abnormal value according to Baseline Limits set by your NNMi administrator. This occurs when any Buffer related metric is abnormal.	Warning
Normal	No incident is generated	The measured value is within the allowable range. NNMi closes any related Abnormal Range incidents.	Normal

Buffer Threshold Incidents

Threshold State Value	Incident	Incident Description	Incident Severity
Low None	Buffer on <*NodeName*> has insufficient capacity or is malfunctioning. Incident Name: `BufferOutOfRangeOrMalfunctioning`	Node Sensor measured a value less than the allowable range according to the Threshold configured by your NNMi administrator and applied to members of a Node Group.	Minor
Nominal	No incident is generated, and current incident changes to Lifecycle State: Closed.	The measured value is within the allowable range. NNMi closes any related High, Low, or None incidents.	Not applicable
High	Buffer on <*NodeName*> has insufficient capacity or is malfunctioning. Incident Name: `BufferOutOfRangeOrMalfunction`	Node Sensor measured a value more than the allowable range according to the Threshold configured by your NNMi administrator and applied to members of a Node Group.	Critical

Buffer Threshold Incidents, continued

Threshold State Value	Incident	Incident Description	Incident Severity
	ing	This occurs when the buffer pool is exhausted or cannot meet demand.	

When buffer Threshold State changes, NNMi updates to the information on the following Incident form tabs:

- Correlated Parents
- Correlated Children
- Custom Attributes

When NNMi determines that the Node Sensor measurement is within the allowable range, NNMi updates the following attributes:

- The Node Sensor Status is changed to **Normal**
- The Node Sensor Conclusion is changed to one of the following:

Buffer Incident's Close Sequence

Node Sensor Conclusion Initiating the Incident	Node Sensor Conclusion Closing the Incident	Node Sensor Status Changes To:
BufferAbnormal	BufferNormal	Normal
BufferOutOfRangeOrMalfunctioning	BufferInRangeAndFunctioning	Normal

This Node Sensor Conclusion propagates to the following:

- "Node Form: Conclusions Tab" on page 95

CPU Incidents (*NNM iSPI Performance for Metrics*)

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

CPU incidents are available if the HPE 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)

The following tables describe the possible results.

CPU Baseline Incidents

Baseline State Value	Incident	Incident Description	Incident Severity
Abnormal Range	CPU on <*NodeName*> is abnormal. Incident Name: `CPUAbnormal`	Node Sensor measured an abnormal value according to Baseline Limits set by your NNMi administrator. Occurs when any CPU related metric is abnormal.	Warning
Normal	No incident is generated	The measured value is within the allowable range. NNMi closes any related Abnormal Range incidents.	Normal

CPU Threshold Incidents

Threshold State Value	Incident	Incident Description	Incident Severity
Low None	CPU on <*NodeName*> utilization is too high. Incident Name: `CpuOutOfRangeOrMalfunctioning`	Node Sensor measured a value less than the allowable range according to the Threshold configured by your NNMi administrator and applied to members of a Node Group.	Minor
Nominal	No incident is generated, and current incident changes to Lifecycle State: Closed.	The measured value is within the allowable range. NNMi closes any related High, Low, or None incidents.	Not applicable
High	CPU on <*NodeName*> utilization is too high. Incident Name: `CpuOutOfRangeOrMalfunctioning`	Occurs when any of 5 second, 1 minute, or 5 minute utilization averages is too high.	Critical

When CPU Threshold State changes, NNMi updates to the information on the following Incident form tabs:

- Correlated Parents
- Correlated Children
- Custom Attributes

When NNMi determines that the Node Sensor is within the allowable range, NNMi updates the following attributes:

- The Node Sensor Status is changed to **Normal**
- The Node Sensor Conclusion is changed to one of the following:

CPU Incident's Close Sequence

Node Sensor Conclusion Initiating the Incident	Node Sensor Conclusion Closing the Incident	Node Sensor Status Changes To:
CPUAbnormal	CPUNormal	Normal
CPUOutOfRangeOrMalfunctioning	CPUInRangeAndFunctioning	Normal

This Node Sensor Conclusion propagates to the following:

- "Node Form: Conclusions Tab" on page 95

Disk Incidents (*NNM iSPI Performance for Metrics*)

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

Disk incidents are available if the HPE 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 NNMi administrator in Monitoring Configuration. 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 following tables describe the possible results.

Disk Baseline Incidents

Baseline State Value	Incident	Incident Description	Incident Severity
Abnormal Range	Disk on <*NodeName*> is abnormal. Incident Name: `DiskAbnormal`	Node Sensor measured an abnormal value according to Baseline Limits set by your NNMi administrator.	Warning
Normal	No incident is generated	The measured value is within the allowable range. NNMi closes any related Abnormal Range incidents.	Normal

Disk Threshold Incidents

Threshold State Value	Incident	Incident Description	Incident Severity
Low None	Disk on <*NodeName*> is out of configured range. Incident Name: `DiskOutOfRangeOrMalfunctioning`	Node Sensor measured a value less than the allowable range according to the Threshold configured by your NNMi administrator and applied to members of a Node Group. This occurs when the disk monitored attributes are out of range.	Minor
Nominal	No incident is generated, and current incident changes to Lifecycle State: Closed.	The measured value is within the allowable range. NNMi closes any related High, Low, or None incidents	Not applicable
High	Disk on <*NodeName*> is out of configured range. Incident Name: `DiskOutOfRangeOrMalfunctioning`	Node Sensor measured a value more than the allowable range according to the Threshold configured by your NNMi administrator and applied to members of a Node Group. This occurs when the disk monitored attributes are out of range.	Critical

When disk Threshold State changes, NNMi updates to the information on the following Incident form tabs:

- Correlated Parents
- Correlated Children
- Custom Attributes

When NNMi determines that the Node Sensor is within the allowable range, NNMi updates the following attributes:

- The Node Sensor Status is changed to **Normal**
- The Node Sensor Conclusion is changed to one of the following:

Disk Incident's Close Sequence

Node Sensor Conclusion Initiating the Incident	Node Sensor Conclusion Closing the Incident	Node Sensor Status Changes To:
DiskAbnormal	DiskNormal	Normal
DiskOutOfRangeOrMalfunctioning	DiskInRangeAndFunctioning	Normal

This Node Sensor Conclusion propagates to the following:

- "Node Form: Conclusions Tab" on page 95

Interface Frame Check Sequence (FCS) Error Rate Incidents (*NNM iSPI Performance for Metrics*)

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

Interface Frame Check Sequence (FCS) error rate incidents are available if the HPE 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 tables describe the possible results.

FCS LAN or FCS WLAN Error Rate Threshold Incidents

Threshold State Value	Incident	Incident Description	Incident Severity
Nominal	No incident is generated, and current incident changes to Lifecycle State: Closed.	The measured value is within the allowable range. NNMi closes any related High, Low, or None incidents.	Not applicable

High	High FCS LAN or FCS WLAN error rate on interface <*ObjectName*>. The $cia.thresholdParameter transitioned from $cia.thresholdPreviousValue to $cia.thresholdCurrentValue due to a measured value of $cia.thresholdMeasuredValue, which is above the configured high value of $cia.thresholdUpperBound. The date and time of the measurement is $cia.thresholdMeasurementTime.
	
	Incident Name:
	`InterfaceFCSLANErrorRateHigh`
	`InterfaceFCSWLANErrorRateHigh`
		Indicates high Frame Check Sequence (FCS) LAN or WLAN error rate, based on the the number of frames that were received with a bad checksum (CRC value). What constitutes an error is system specific, but likely includes such issues as collisions at half-duplex, a duplex mismatch, bad hardware (NIC, cable, or port), or a connected device generating frames with bad FCS.	Critical

When Threshold State changes, NNMi updates to the information on the following Incident form tabs:

- Correlated Parents
- Correlated Children
- Custom Attributes

When NNMi determines that the FCS LAN Interface Error Rate or FCS WLAN 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:

FCS LAN or FCS WLAN Error Rate Threshold Incident's Close Sequence

Interface Conclusion Initiating the Incident	Interface Conclusion Closing the Incident	Interface Status Changes To:
InterfaceFCSLANErrorRateHigh	InterfaceFCSLANErrorRateInRange	Normal
InterfaceFCSWLANErrorRateHigh	InterfaceFCSWLANErrorRateInRange	Normal

This Interface Conclusion propagates to the following:

- "Layer 2 Connection Form: Conclusions Tab" on page 260
- "Node Form: Conclusions Tab" on page 95

Interface Input and Output Discard Rate Incidents (*NNM iSPI Performance for Metrics*)

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

Interface input and output discard rate incidents are available if the HPE 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.

The following tables describe the possible results.

Interface Input and Output Discard Rate Threshold Incidents

Threshold State Value	Incident	Incident Description	Incident Severity
Nominal	No incident is generated, and current incident changes to Lifecycle State: Closed.	The measured value is within the allowable range. NNMi closes any related High, Low, or None incidents.	Not applicable

High	High input or output discard rate on interface $sourceObjectName. The $cia.thresholdParameter transitioned from $cia.thresholdPreviousValue to $cia.thresholdCurrentValue due to a measured value of $cia.thresholdMeasuredValue, which is between the configured low value of $cia.thresholdLowerBound and the configured high value of $cia.thresholdUpperBound. The date and time of the measurement is $cia.thresholdMeasurementTime.
	
	Incident Name:
	`InterfaceInputDiscardRateHigh`
	
	`InterfaceOutputDiscardRateHigh`
		Indicates high input or output discard rate, based on the reported change in the number of output packets on the interface and the discarded packet count. Packets may be discarded because of a variety of issues, including receive buffer overflows, congestion, or system specific issues.	Major

When Threshold State changes, NNMi updates to the information on the following Incident form tabs:

- Correlated Parents
- Correlated Children
- Custom Attributes

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 Conclusion is changed as shown in the following table:

Interface Input and Output Discard Rate Incident's Close Sequence

Interface Conclusion Initiating the Incident	Interface Conclusion Closing the Incident	Interface Status Changes To:
InterfaceInputDiscardRateHigh	InterfaceInputDiscardRateNominal	Normal
InterfaceOutputDiscardRateHigh	InterfaceOutputDiscardRateNominal	Normal

This Interface Conclusion propagates to the following:

- "Layer 2 Connection Form: Conclusions Tab" on page 260
- "Node Form: Conclusions Tab" on page 95

Interface Input and Output Error Rate Incidents (*NNM iSPI Performance for Metrics*)

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

Interface input and output error rate incidents are available if the HPE 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.

The following tables describe the possible results.

Interface Input and Output Error Rate Threshold Incidents

Threshold State Value	Incident	Incident Description	Incident Severity
Nominal	No incident is generated	The measured value is within the allowable range. NNMi closes any related High incidents.	Not applicable
High	High input or output error rate on interface <*ObjectName*>. The $cia.thresholdParameter transitioned from $cia.thresholdPreviousValue to $cia.thresholdCurrentValue due to a measured value of $cia.thresholdMeasuredValue, which is between the configured low value of $cia.thresholdLowerBound and the configured high value of $cia.thresholdUpperBound. The date and time of the measurement is $cia.thresholdMeasurementTime. Incident Name:	Indicates high input or output error rate, based on the reported change in the number of input or output packets on the interface and the packet error count. What constitutes an error is system specific, but likely includes such issues as bad packet checksums, incorrect header information, runt packets, etc.	Critical

Interface Input and Output Error Rate Threshold Incidents, continued

Threshold State Value	Incident	Incident Description	Incident Severity
	`InterfaceInputErrorRateHigh` `InterfaceOutputErrorRateHigh`		

When Threshold State changes, NNMi updates to the information on the following Incident form tabs:

- Correlated Parents
- Correlated Children
- Custom Attributes

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:

Interface Input and Output Error Rate Threshold Incident's Close Sequence

Interface Conclusion Initiating the Incident	Interface Conclusion Closing the Incident	Interface Status Changes To:
InterfaceInputErrorRateHigh	InterfaceInputErrorRateNominal	Normal
InterfaceOutputErrorRateHigh	InterfaceOutputErrorRateNominal	Normal

This Interface Conclusion propagates to the following:

- "Layer 2 Connection Form: Conclusions Tab" on page 260
- "Node Form: Conclusions Tab" on page 95

Input and Output Queue Drop Incidents (*NNM iSPI Performance for Metrics*)

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

Input Queue Drop and Output Queue Drop incidents are available if the HPE 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 tables describe the possible results.

Interface Input and Output Queue Drop Threshold Incidents

Threshold State Value	Incident	Incident Description	Incident Severity
Nominal	No incident is generated	The measured value is within the allowable range. NNMi closes any related High incidents.	Not applicable

High	High input or output queue drops rate on interface $sourceObjectName. The $cia.thresholdParameter transitioned from $cia.thresholdPreviousValue to $cia.thresholdCurrentValue due to a measured value of $cia.thresholdMeasuredValue, which is between the configured low value of $cia.thresholdLowerBound and the configured high value of $cia.thresholdUpperBound. The date and time of the measurement is $cia.thresholdMeasurementTime.
	
	Incident Name:
	`InterfaceInputQueueDropsRateHigh`
	`InterfaceOutputQueueDropsRateHigh`
		Indicates high input or output queue drops rate, based on the number of packets dropped because of a full queue. What constitutes an error is system specific, but likely includes such issues as the number of packet buffers allocated to the interface is exhausted or reaches its maximum threshold.	Major

When Threshold State changes, NNMi updates to the information on the following Incident form tabs:

- Correlated Parents
- Correlated Children
- Custom Attributes

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:

Interface Input and Output Queue Drop Threshold Incident's Close Sequence

Interface Conclusion Initiating the Incident	Interface Conclusion Closing the Incident	Interface Status Changes To:
InterfaceInputQueueDropsHigh	InterfaceInputQueueDropsRateInRange	Normal
InterfaceOutputQueueDropsHigh	InterfaceOutputQueueDropsRateInRange	Normal

Potential propagation influence on other objects as follows:

- "Layer 2 Connection Form: Conclusions Tab" on page 260
- "Node Form: Conclusions Tab" on page 95

Interface Input and Output Utilization Incidents (*NNM iSPI Performance for Metrics*)

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

Input and output utilization incidents are available if the HPE 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 tables describe the possible results.

Interface Baseline Incidents

Baseline State Value	Incident	Incident Description	Incident Severity
Abnormal Range	Abnormal input or output utilization on interface <*ObjectName*>. Incident Name: `InterfaceInputUtilizationAbnormal`	Indicates abnormal input or output utilization, based on the interface speed, and the reported change in the number of input or output bytes on the interface. The exact MIB values queried varies based on the speed of	Warning

Interface Baseline Incidents, continued

Baseline State Value	Incident	Incident Description	Incident Severity
	`InterfaceOutputUtilizationAbnormal`	the interface and whether the system supports the high speed counters for interfaces.	
Normal	No incident is generated	The measured value is within the allowable range. NNMi closes any related Abnormal Range incidents.	Normal

The following table describes the meaning of the threshold range measurements of None, Low, Nominal, and High:

Interface Threshold Incidents

Threshold State Value	Incident	Incident Description	Incident Severity

None	Zero input or output utilization on interface <*ObjectName*>. The $cia.thresholdParameter transitioned from $cia.thresholdPreviousValue to $cia.thresholdCurrentValue due to a measured value of $cia.thresholdMeasuredValue. The date and time of the measurement is $cia.thresholdMeasurementTime.
	
	Incident Name:
	`InterfaceInputUtilizationLow`
	`InterfaceOutputUtilizationLow`
		Indicates zero input or output utilization, based on the interface speed, and the reported change in the number of input or output bytes on the interface. The exact MIB values queried varies based on the speed of the interface and whether the system supports the high speed counters for interfaces.	Minor

Low	Low input or output utilization on interface <*ObjectName*>. The $cia.thresholdParameter transitioned from $cia.thresholdPreviousValue to $cia.thresholdCurrentValue due to a measured value of $cia.thresholdMeasuredValue, which is between the minimum allowed value of $cia.thresholdLowerBound and the configured low value of $cia.thresholdUpperBound. The date and time of the measurement is $cia.thresholdMeasurementTime.
	
	Incident Name:
	`InterfaceInputUtilizationNone`
	`InterfaceOutputUtilizationNone`
		Indicates low input utilization, based on the interface speed, and the reported change in the number of input or output bytes on the interface. The exact MIB values queried varies based on the speed of the interface and whether the system supports the high speed counters for interfaces.	Major

Interface Threshold Incidents, continued

Threshold State Value	Incident	Incident Description	Incident Severity
Nominal	No incident is generated	The measured value is within the allowable range. NNMi closes any related High, Low, or None incidents.	Normal

High	High input or output utilization on interface $sourceObjectName. The $cia.thresholdParameter transitioned from $cia.thresholdPreviousValue to $cia.thresholdCurrentValue due to a measured value of $cia.thresholdMeasuredValue, which is between the configured high value of $cia.thresholdLowerBound and the maximum allowed value of $cia.thresholdUpperBound. The date and time of the measurement is $cia.thresholdMeasurementTime.
	
	Incident Name:
	`InterfaceInputUtilizationHigh`
	`InterfaceOutputUtilizationHigh`
		Indicates high input or output utilization, based on the interface speed, and the reported change in the number of input or output bytes on the interface. The exact MIB values queried varies based on the speed of the interface and whether the system supports the high speed counters for interfaces.	Major

When Threshold State changes, NNMi updates to the information on the following Incident form tabs:

- Correlated Parents
- Correlated Children
- Custom Attributes

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:

Interface Baseline Incident's Close Sequence

Interface Conclusion Initiating the Incident	Interface Conclusion Closing the Incident	Interface Status Changes To:
InterfaceInputUtilizationAbnormal	InterfaceOutputUtilizationNormal	Normal
InterfaceOutputUtilizationAbnormal	InterfaceOutputUtilizationNormal	Normal

Interface Threshold Incident's Close Sequence

Interface Conclusion Initiating the Incident	Interface Conclusion Closing the Incident	Interface Status Changes To:
InterfaceInputUtilizationNone	InterfaceInputUtilizationNominal	Normal
InterfaceInputUtilizationLow	InterfaceInputUtilizationNominal	Normal
InterfaceInputUtilizationHigh	InterfaceOutputUtilizationNominal	Normal
InterfaceOutpuUtilizationNone	InterfaceOutputUtilizationNominal	Normal
InterfaceOutputUtilizationLow	InterfaceOutputUtilizationNominal	Normal
InterfaceOutputUtilizationHigh	InterfaceOutputUtilizationNominal	Normal

This Interface Conclusion propagates to the following:

- "Layer 2 Connection Form: Conclusions Tab" on page 260
- "Node Form: Conclusions Tab" on page 95

Management Address ICMP Response Time Incidents

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

Management Address ICMP Response Time incidents are available if your administrator configured performance measurement thresholds (HPE Network Node Manager iSPI Performance for Metrics Software is not required for this threshold). For more information:).

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 tables describe the possible results.

Management Address ICMP Response Time Baseline Incidents

Baseline State Value	Incident	Incident Description	Incident Severity
Abnormal	Abnormal ICMP response time from the management server to node <*NodeName*>. Incident Name: `ManagementAddressICMPResponseTimeAbnormal`	Indicates abnormal Internet Control Message Protocol (ICMP) response time from the management server to the target node. ICMP messages are typically used for diagnostic or routing purposes for determining whether a host or router could not be reached. The incident is generated when NNMi detects a higher than configured ICMP response time between the management server and the target node.	Warning
Normal	No incident is generated	The measured value is within the allowable range. NNMi closes any related Abnormal Range incidents.	Normal

Management Address ICMP Response Time Threshold Incidents

Threshold State Value	Incident	Incident Description	Incident Severity
Nominal	No incident is generated, and current incident changes to Lifecycle State: Closed.	The measured value is within the allowable range. NNMi closes any related High incidents.	Not applicable
High	High ICMP response time from the management server to node <*NodeName*>. The $cia.thresholdParameter transitioned from $cia.thresholdPreviousValue to $cia.thresholdCurrentValue due to a measured value of $cia.thresholdMeasuredValue, which is between the lower bound of $cia.thresholdLowerBound and the upper bound of $cia.thresholdUpperBound. The date and time of the measurement is $cia.thresholdMeasurementTime. Incident Name:	Indicates high Internet Control Message Protocol (ICMP) response time from the management server to the target node. ICMP messages are typically used for diagnostic or routing purposes for determining whether a host or router could not be reached. The incident is generated when NNMi detects a higher than configured ICMP response time between the management server and the target node.	Warning

Management Address ICMP Response Time Threshold Incidents, continued

Threshold State Value	Incident	Incident Description	Incident Severity
	ManagementAddressICMPResponseTimeHigh		

When management address ICMP response time threshold State changes, NNMi updates to the information on the following Incident form tabs:

- Correlated Parents
- Correlated Children
- Custom Attributes

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:

Management Address ICMP Response Time Incident's Close Sequence

SNMP Agent Conclusion Initiating the Incident	SNMP Agent Conclusion Closing the Incident	SNMP Agent Status Changes To:
ManagementAddressICMPResponseTimeAbnormal	ManagementAddressICMPResponseTimeNormal	Normal
ManagementAddressICMPResponseTimeHigh	ManagementAddressICMPResponseTimeNominal	Normal

This SNMP Agent Conclusion propagates to the following:

- "Node Form: Conclusions Tab" on page 95

Memory Incidents (*NNM iSPI Performance for Metrics*)

Requires HPE Network Node Manager iSPI Performance for Metrics Software (NNM iSPI Performance for Metrics). To populate performance data in the dashboard views or enhance NNM iSPI Performance for Metrics reports by sharing NNMi configuration settings, install the *optional* Network Performance Server (NPS) -- click here for more information.

Memory incidents are available if the HPE 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 tables describes the possible results.

Memory Baseline Incidents

Baseline State Value	Incident	Incident Description	Incident Severity
Abnormal Range	Memory on <*NodeName*> is abnormal. Incident Name: `MemoryAbnormal`	Node Sensor measured an abnormal value according to Baseline Limits set by your NNMi administrator. This occurs when any Memory related metric is abnormal.	Warning
Normal	No incident is generated	The measured value is within the allowable range. NNMi closes any related Abnormal Range incidents.	Normal

Memory Threshold Incidents

Threshold State Value	Incident	Incident Description	Incident Severity
Low None	Memory on <*NodeName*> has insufficient capacity or is malfunctioning. Incident Name: `MemoryOutOfRangeOrMalfunctioning`	Node Sensor measured a value less than the allowable range according to the Threshold configured by your NNMi administrator and applied to members of a Node Group.	Minor
Nominal	No incident is generated, and current incident changes to Lifecycle State: Closed.	The measured value is within the allowable range. NNMi closes any related High, Low, or None incidents.	Not applicable
High	Memory on <*NodeName*> has insufficient capacity or is malfunctioning. Incident Name: `MemoryOutOfRangeOrMalfunctioning`	Node Sensor measured a value more than the allowable range according to the Threshold configured by your NNMi administrator and applied to members of a Node Group. This occurs when the memory pool is exhausted or cannot meet demand.	Critical

When memory Threshold State changes, NNMi updates to the information on the following Incident form tabs:

- Correlated Parents
- Correlated Children
- Custom Attributes

When NNMi determines that the Node Sensor is within the allowable range, NNMi updates the following attributes:

- The Node Sensor Status is changed to **Normal**.
- The Node Sensor Conclusion is changed to one of the following:

Memory Incident's Close Sequence

Node Sensor Conclusion Initiating the Incident	Node Sensor Conclusion Closing the Incident	Node Sensor Status Changes To:
MemoryAbnormal	MemoryDiskNormal	Normal
MemoryOutOfRangeOrMalfunctioning	MemoryInRangeAndFunctioning	Normal

This Node Sensor Conclusion propagates to the following:

- "Node Form: Conclusions Tab" on page 95

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 409 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	The current value of the *fully-qualified, case-sensitive* Hostname attribute as it appears on the Node form. 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. • 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). When the NNMi administrator chooses **Enable SNMP Address Rediscovery** ☑ in

"Find Node" Options, continued

Possible Values	Description
	the Communication Configuration: ◦ If the SNMP Agent does not respond, NNMi checks for another Management Address to request the Hostname, and the Hostname could change. ◦ If the SNMP Agent associated with the node changes, the Management Address and Hostname could change. When the NNMi administrator disables **Enable SNMP Address Rediscovery** ☐ in the Communication Configuration, when the current management address (SNMP agent) becomes unreachable, NNMi does not check for other potential management addresses. • 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. **Note:** NNMi administrators can use NNMi property file settings to change the way NNMi determines Hostname values: • `nms-topology.properties` 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 *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`. • `nms-disco.properties` 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 *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.
IP address of any interface	The IP address of any interface in the node.
System Name	The current value of the MIB-II `sysName` that is obtained from the node's SNMP agent (case-sensitive) as it appears in the System Name attribute on Node form. For example

"Find Node" Options, continued

Possible Values	Description
	`cisco5500.abc.example.com`
Name	The current value of the Name attribute as it appears on the Node form. The NNMi administrator configures how NNMi populates this attribute through two configuration settings: (1) The **Node Name Resolution** attributes in Discovery Configuration (full or short DNS name, full or short sysName, IP address). (2) The Name *might be* converted to all uppercase or all lowercase (depending on how the NNMi administrator configured settings in the `nms-topology.properties` file). See the "Modifying NNMi Normalization Properties" section of the *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.

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	The End Node's *fully-qualified, case-sensitive* Hostname value. The End Node can be either of the following: • A device in your network environment that has not been discovered by NNMi (no corresponding Node object in the NNMi database). • A Node previously discovered by NNMi. The Hostname you provide must match the current *case-sensitive* value of the end Node's *Hostname* attribute on the "Node Form" on page 65. See "Access Node Details" on page 409 and Access More Details (Forms and Analysis Pane) for methods of looking up the current Hostname value. 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. ◦ 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). When the NNMi administrator chooses **Enable SNMP Address Rediscovery** ☑ in the Communication Configuration: • If the SNMP Agent does not respond, NNMi checks for another Management Address to request the Hostname, and the Hostname could change. • If the SNMP Agent associated with the node changes, the Management Address and Hostname could change. When the NNMi administrator disables **Enable SNMP Address Rediscovery** ☐ in the Communication Configuration, when the current management address (SNMP agent) becomes unreachable, NNMi does not check for other potential management addresses. ◦ 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. **Note:** NNMi administrators can use NNMi property file settings to change the way NNMi determines Hostname values: ◦ `nms-topology.properties` 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

"Find Attached Switch Port" Options, continued

Possible Values	Description
	all lowercase. See the "Modifying NNMi Normalization Properties" section of the *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`. ◦ `nms-disco.properties` 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 *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.
IP address of any interface	The current value of any IP address associated with the End Node. (*NNMi Advanced*.) 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.

When using this feature, note the following:

- To ensure that NNMi is using the most current data available for its analysis, first use nnmconfigpoll.ovpl on the switch for which you want to view end node information.
- Only one node must be available on a port for the node to qualify as an end node. This can be an issue when managing Voice Over IP phones that are also attached to lap top computers. If both devices respond as a node on the same port, neither device is reported.
- The SNMP information that NNMi has available for its analysis depends upon the switch activity. For example, if an end node has not had recent activity on the switch, it might not have the required SNMP data available for NNMi to include the node in the results. This means that results of **Show Attached End Nodes** might vary in time.

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 also right-click any object in a table or map view to access the items available within 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:

- 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 571

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 also right-click any object in a table or map view to access the items available within 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 *HPE Network Node Manager i Software Deployment Reference*, which is available at: `http://softwaresupport.hpe.com`.

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

HPE Network Node Manager i Software Deployment Reference, which is available at: `http://softwaresupport.hpe.com`.

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 382 for more information.
- The starting node is the NNMi management server on which you are running the traceroute command.

Tip: You can also right-click any object in a table or map view to access the items available within 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 *HPE 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 also right-click any object in a table or map view to access the items available within 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 56 or "Node Groups View (Monitoring)" on page 403).
  b. Select the row representing the Node Group of interest.
  c. Select **Actions** → **Status Details**.

  > **Tip:** You can also right-click any object in a table or map view to access the items available within 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 37 for more information about filtering views using Node Groups.

Chapter 13: Viewing Lists of the Unmanaged Objects in Your Network

NNMi provides the Management Mode workspace so you can quickly see lists of unmanaged nodes, interfaces, IP addresses, chassis, cards, node sensors, or physical sensors.

For more information about these views:

- Unmanaged Nodes View 581
- Unmanaged Interfaces View 582
- Unmanaged IP Addresses View 583
- Unmanaged Chassis View 583
- Unmanaged Cards View 584
- Unmanaged Node Sensors View 585
- Unmanaged Physical Sensors View 585
- Scheduled Node Outages View 586
- Stop or Start Managing an Object 587

The object might be unmanaged because of either of the following:

- "How NNMi Assigns the Management Mode to an Object" on page 591
- "How NNMi Users Change a Management Mode" on page 592

See also "Understand the Effects of Setting the Management Mode to Not Managed or Out of Service" on page 589.

Unmanaged Nodes View

Tip: See "Node Form" on page 65 for more information about the attributes that appear in each column in this view.

The **Unmanaged Nodes** view in the Management Mode workspace identifies all of the nodes with a management mode of either **Not Managed** or **Out of Service**. These are the nodes that are no longer being discovered or monitored. This includes nodes currently participating in a scheduled outage ("Scheduled Node Outages View" on page 586).

Use this view to select nodes and change the Management Mode to **Managed**.

To display the Unmanaged Nodes view:

1. In the **Workspaces** navigation pane, select the **Management Mode** workspace.
2. Select the **Unmanaged Nodes** view.

For each node, you can identify its overall status (for example, **Normal**, **Warning**, **Minor**, **Major**, **Critical** and **Unknown**), device category (for example, switch), Node Management Mode, name, system name, management address, system location (the current value of the sysLocation MIB variable), device profile, whether the SNMP Agent is enabled, the date and time the status was last modified, and any notes included for the node.

See "Nodes View (Inventory)" on page 38 for more information about uses for nodes views.

Related Topics

"Understand the Effects of Setting the Management Mode to Not Managed or Out of Service" on page 589

"How NNMi Users Change a Management Mode" on page 592

"How NNMi Assigns the Management Mode to an Object" on page 591

"Viewing Lists of the Unmanaged Objects in Your Network" on the previous page

Unmanaged Interfaces View

Tip: See "Interface Form" on page 113 for more information about the attributes that appear in each column in this view.

The **Unmanaged Interfaces** view in the Management Mode workspace identifies all of the interfaces with a Management Mode of either **Not Managed** or **Out of Service**. These are the interfaces that are no longer being discovered or monitored. This includes interfaces currently affected by a scheduled outage ("Scheduled Node Outages View" on page 586).

Use this view to select interfaces and change the Management Mode to **Managed**.

To display the Unmananaged Interfaces view:

1. In the **Workspaces** navigation pane, select the **Management Mode** workspace.
2. Select the **Unmanaged Interfaces** view.

For each interface, you can identify the interface's overall status (for example, **Normal**, **Warning**, **Minor, Major, Critical**, and **Unknown**), administrative state, operational state, the management mode of the interface, the management mode of the associated node, the node on which the interface resides (Hosted on Node), the interface name, type, speed, index, description, and alias, the date the interface status and state was last changed, and any notes included for the interface.

See "Interfaces View (Inventory)" on page 39 for more information about uses for the interfaces views.

Related Topics

"Understand the Effects of Setting the Management Mode to Not Managed or Out of Service" on page 589

"How NNMi Users Change a Management Mode" on page 592

"How NNMi Assigns the Management Mode to an Object" on page 591

"Viewing Lists of the Unmanaged Objects in Your Network" on the previous page

Unmanaged IP Addresses View

Tip: See "IP Address Form" on page 160 for more information about the attributes that appear in each column in this view.

The **Unmanaged Addresses** view in the Management Mode workspace identifies all of the addresses with a Management Mode of either **Not Managed** or **Out of Service**. These are the addresses that are no longer being discovered or monitored. This includes IP addresses currently affected by a scheduled outage ("Scheduled Node Outages View" on page 586).

Use this view to select addresses and change the Management Mode to **Managed**.

To display the Unmananaged IP Addresses view:

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

For each IP address, you can identify its status, state, management mode, interface direct management mode, the management mode of its associated node, the IP address value, the name of the interface on which the address resides (**In Interface**), the name of the node on which the address resides (**Hosted on Node**), subnet (**In Subnet**) and prefix length (**PL**), the date and time in which the status was last modified, and any notes included for the IP address.

See "IP Addresses View (Inventory)" on page 41 for more information about uses for address views.

Related Topics

"Understand the Effects of Setting the Management Mode to Not Managed or Out of Service" on page 589

"How NNMi Users Change a Management Mode" on page 592

"How NNMi Assigns the Management Mode to an Object" on page 591

"Viewing Lists of the Unmanaged Objects in Your Network" on page 581

Unmanaged Chassis View

Tip: See "Chassis Form" on page 193 for more information about the attributes that appear in each column in this view.

The **Unmanaged Chassis** view in the Management Mode workspace identifies all of the chassis with a Management Mode of either **Not Managed** or **Out of Service**. These are the chassis that are no longer being discovered or monitored. This includes chassis currently affected by a scheduled outage ("Scheduled Node Outages View" on page 586).

Use this view to select chassis and change the Management Mode to **Managed**.

To display the Unmanaged Chassis view:

1. In the **Workspaces** navigation pane, select the **Management Mode** workspace.
2. Select the **Unmanaged Chassis** view.

For each chassis, you can identify its status, management mode, the management mode of the node on which it resides, the administrative state, the operational state, the name of the node using the chassis (**Managed By**), the date and time the status was last modified, its name, model, type, serial number, firmware version, hardware version, software version, index, the name of the chassis on which the chassis resides, if any, any Redundant Group to which the chassis belongs, the date and time the state was last modified, the chassis Description, and any notes included for the chassis.

See "Chassis View" on page 45 for more information about uses for chassis views.

Related Topics

"Understand the Effects of Setting the Management Mode to Not Managed or Out of Service" on page 589

"How NNMi Users Change a Management Mode" on page 592

"How NNMi Assigns the Management Mode to an Object" on page 591

"Viewing Lists of the Unmanaged Objects in Your Network" on page 581

Unmanaged Cards View

Tip: See "Card Form" on page 211 for more information about the attributes that appear in each column in this view.

The **Unmanaged Cards** view in the Management Mode workspace identifies all of the cards with a Management Mode of either **Not Managed** or **Out of Service**. These are the cards that are no longer being discovered or monitored. This includes cards currently affected by a scheduled outage ("Scheduled Node Outages View" on page 586).

Use this view to select cards and change the Management Mode to **Managed**.

To display the Unmanaged Cards view:

1. In the **Workspaces** navigation pane, select the **Management Mode** workspace.
2. Select the **Unmanaged Cards** view.

For each card, you can identify its status, management mode, the management mode of the node on which it resides, the administrative state, the operational state, the name of the node using that Card (**Managed By**), the date and time the status was last modified, its name, model, type, serial number, firmware version, hardware version, software version, index, the name of the card on which the card resides, if any, any Redundant Group to which the card belongs, the date and time the state was last modified, the card Description, and any notes included for the card.

See "Cards View" on page 46 for more information about uses for card views.

Related Topics

"Understand the Effects of Setting the Management Mode to Not Managed or Out of Service" on page 589

"How NNMi Users Change a Management Mode" on page 592

"How NNMi Assigns the Management Mode to an Object" on page 591

"Viewing Lists of the Unmanaged Objects in Your Network" on page 581

Unmanaged Node Sensors View

Tip: See "Node Sensor Form" on page 232 for more details about the node sensor attributes that appear in this view's column headings. Node Sensors are displayed in three views: "Node Sensors View" on page 47, "Non-Normal Node Sensors View" on page 393, and "Unmanaged Node Sensors View" above.

The **Unmanaged Node Sensors** view in the Management Mode workspace identifies all of the Node Sensors with a Direct Management Mode of either **Not Managed** or **Out of Service**. These are the Node Sensors that are no longer being discovered or monitored. This includes node sensors currently affected by a scheduled outage ("Scheduled Node Outages View" on the next page).

Use this view to select Node Sensors and change the Direct Management Mode to **Inherited**.

To display the Unmanaged Node Sensors view:

1. In the **Workspaces** navigation pane, select the **Management Mode** workspace.
2. Select the **Unmanaged Node Sensors** view.

For each Node Sensor, you can identify its Status, Direct Management Mode, the Management Mode of the node on which it resides, its Name, type, the name of the node on which it resides (**Hosted On Node**), and the date and time the Status was last modified.

See "Non-Normal Node Sensors View" on page 393 for more information about uses for node sensor views.

Related Topics

"Understand the Effects of Setting the Management Mode to Not Managed or Out of Service" on page 589

"How NNMi Users Change a Management Mode" on page 592

"How NNMi Assigns the Management Mode to an Object" on page 591

"Viewing Lists of the Unmanaged Objects in Your Network" on page 581

Unmanaged Physical Sensors View

Tip: See "Physical Sensor Form" on page 244 for more details about the node sensor attributes that appear in this view's column headings. Node Sensors are displayed in three views: "Physical Sensors View" on page 47, "Non-Normal Physical Sensors View" on page 394, and Unmanaged Physical Sensors View.

The **Unmanaged Physical Sensors** view in the Management Mode workspace identifies all of the Physical Sensors with a Direct Management Mode of either **Not Managed** or **Out of Service**. These are the Physical Sensors that are no longer being discovered or monitored. This includes physical sensors currently affected by a scheduled outage ("Scheduled Node Outages View" on the next page).

Use this view to select Physical Sensors and change the Direct Management Mode to **Inherited**.

To display the Unmanaged Physical Sensors view:

1. In the **Workspaces** navigation pane, select the **Management Mode** workspace.
2. Select the **Unmanaged Physical Sensors** view.

For each Physical Sensor, you can identify its Status, Direct Management Mode, the Management Mode of the node on which it resides, its Name, type, the name of the node on which it resides (**Hosted On Node**), and the date and time the Status was last modified.

See "Non-Normal Physical Sensors View" on page 394 for more information about uses for node sensor views.

Related Topics

"Understand the Effects of Setting the Management Mode to Not Managed or Out of Service" on page 589

"How NNMi Users Change a Management Mode" on page 592

"How NNMi Assigns the Management Mode to an Object" on page 591

"Viewing Lists of the Unmanaged Objects in Your Network" on page 581

Scheduled Node Outages View

Tip: See "Scheduling Outages for Nodes or Node Groups" on page 322 for more information about the attributes that appear in each column in this view. For the alternate method of configuring a Scheduled Node Outage, see the nnmscheduledoutage.ovpl Reference Page.

The **Scheduled Node Outages** view in the Management Mode workspace provides a record of all past, present, and future Scheduled Node Outages.

To display the Scheduled Node Outages view:

1. In the **Workspaces** navigation pane, select the **Management Mode** workspace.
2. Select the **Scheduled Node Outages** view.

During the Scheduled Outage time period, NNMi suspends any Discovery and Monitoring of that Node and changes the following:

- Node Status = **No Status**
- Node Management Mode = **Out of Service**

When the specified time period ends, NNMi gathers current information and updates the Node data.

See "Understand the Effects of Setting the Management Mode to Not Managed or Out of Service" on page 589.

Note: You cannot modify a past or current Scheduled Outage. NNMi administrators and Level 2 Operators can delete an inaccurate past record and create a new past Scheduled Outage (see "Scheduling Outages for Nodes or Node Groups" on page 322).

Stop or Start Managing an Object

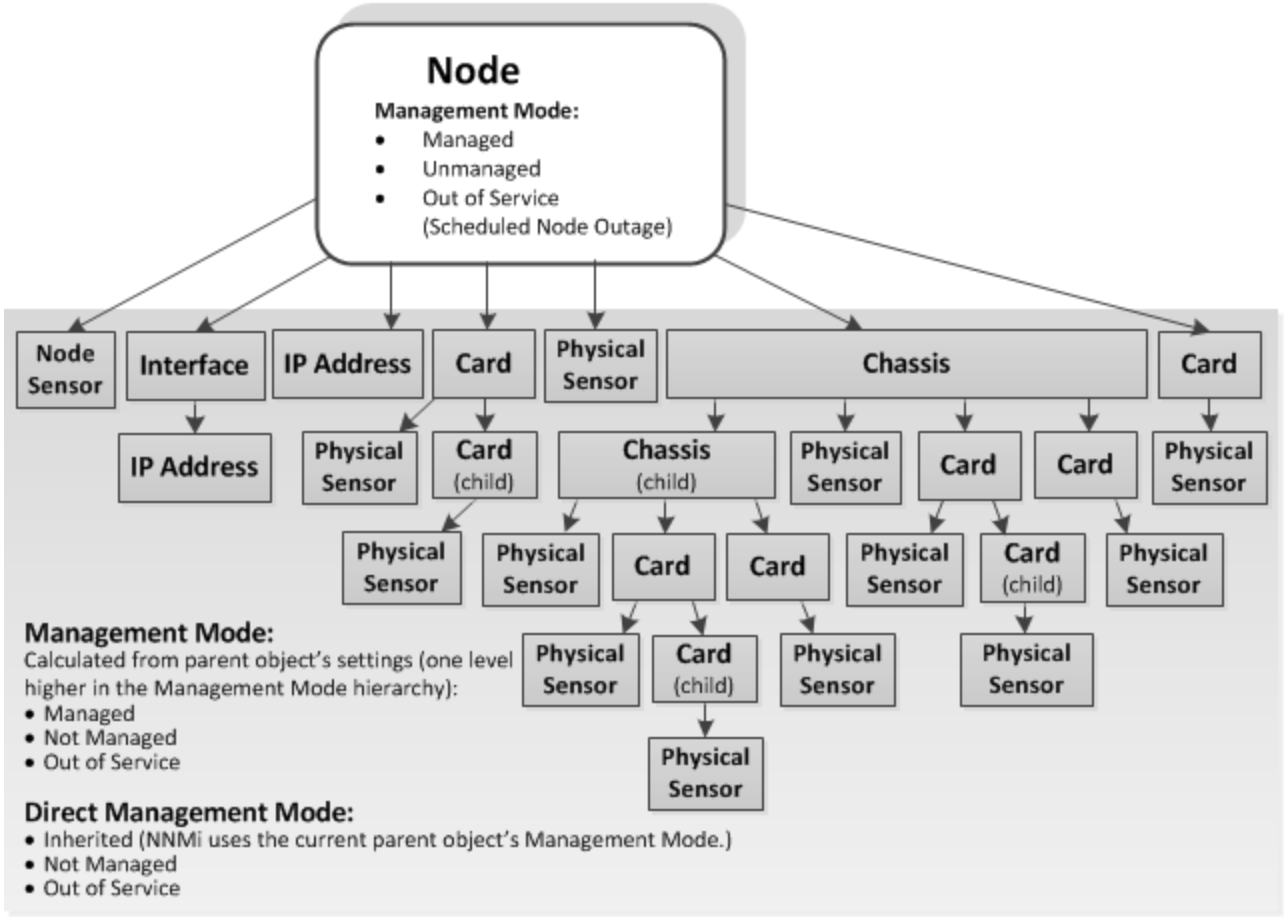
NNMi administrators or Level 2 Operators can specify that a node, interface, IP address, chassis, card, node sensor, or physical sensor should not be discovered or monitored. For additional information see the form for each object:

Reasons you might want to change the Management Mode include:

- Unmanaged = You determine that NNMi should never monitor a particular node, interface, chassis, card, IP address, node sensor, or physical sensor.
- Out of Service = You manually set the node to out of service or schedule a node outage for a particular block of time.

The following illustration shows the possibilities for the influence of Management Mode settings.

Hierarchy of Management Mode Settings



NNMi provides one level of management mode for nodes and two levels of management mode settings for other object types: (as described in the table).

Management Modes

Name	Description
Node Management Mode	For Node objects, this value is set by the NNMi administrator. The Node Management Mode affects other objects in the hierarchy associated with that node. Possible values include: **Managed** - Indicates that NNMi can discover and monitor the Node and associated objects lower in the object hierarchy. **Not Managed** - Indicates that NNMi should not discover or monitor the Node nor the associated objects lower in the object hierarchy. For example, the object might not be accessible because it is in a private network. **Out of Service** - Indicates a Node is out of service. NNMi does not discover or monitor the Node nor the associated objects lower in the hierarchy. **Tip:** To change the Node Management Mode back to **Managed**, right-click the Node in a table or map view and select: **Management Mode** → **Managed (Reset All)** to manage all associated objects in the hierarchy. **Management Mode** → **Managed** to maintain any manually configured Direct Management Mode settings for associated objects in the hierarchy.
Management Mode	Appears on the forms of interface, IP address, chassis, card, node sensor, or physical sensors. This value is calculated by NNMi from the settings higher in the hierarchy: **Managed** **Not Managed** **Out of Service**
Direct Management Mode	Setting provided for interfaces, IP addresses, chassis, cards, node sensors, or physical sensors. NNMi uses this value to compute the Management Mode of this object and any other objects below this object in the hierarchy. This value can be set by the NNMi administrator. Possible values include: **Inherited** - NNMi calculated the Direct Management Mode from settings for objects higher up the management hierarchy. **Not Managed** - Indicates that NNMi should not discover or monitor the object nor the associated objects lower in the hierarchy. For example, the object might not be accessible because it is in a private network. **Out of Service** - Indicates an object is out of service. NNMi does not discover or monitor the object nor the associated objects lower in the hierarchy. **Tip:** To change the Direct Management Mode back to **Inherited**, right-click the object

Management Modes, continued

Name	Description
	in a table or map view and select: **Management Mode** → **Managed (Reset All)** to allow NNMi to manage all associated objects lower in the hierarchy. **Management Mode** → **Managed** to maintain any manually configured Direct Management Mode settings for associated objects lower in the hierarchy.

For more information, see the following topics:

- "Understand the Effects of Setting the Management Mode to Not Managed or Out of Service" below
- "How NNMi Assigns the Management Mode to an Object" on page 591
- "How NNMi Users Change a Management Mode" on page 592
- "Scheduling Outages for Nodes or Node Groups" on page 322

See also "Viewing Lists of the Unmanaged Objects in Your Network" on page 581.

Understand the Effects of Setting the Management Mode to Not Managed or Out of Service

NNMi administrators or Level 2 Operators can instruct NNMi to no longer manage a node, interface, card, address, node sensor, or physical sensor by selecting a *Management Mode* value on the object's form or by using **Actions** → **Management Mode** or by configuring a Scheduled Outage.

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

The results of setting the management mode to **Not Managed** or **Out of Service** for an object, depends on whether you are setting the value for a node, interface, address, card, node sensor, or physical sensor:

- **Nodes: Management Mode**

  For nodes, setting the Management Mode to **Not Managed** or **Out of Service** has the following effects:
  - No incidents are generated for the node
  - The node's SNMP Agent is excluded from fault polling.
  - All monitored objects associated with the node are excluded from fault and performance polling.
  - The Active State for any Custom Poller Nodes associated with the **Not Managed** or **Out of Service** node becomes **Inactive**.
  - Traps related to the node, interface, card, address, node sensor, or physical sensor (for example, coldStart or warmStart) are not stored.

- The node is excluded from discovery.
- **Actions → Polling → Configuration Poll** is no longer available for this node.
- The status of the node is set to **No Status**.
- **Actions → Polling → Status Poll** is no longer available for the node or incident related to that node.

- **Interfaces: Direct Management Mode**

  For interfaces, setting the Direct Management Mode to **Not Managed** or **Out of Service** has the following effects:
  - No incidents are generated for the interface.
  - The interface and any related addresses are excluded from fault and performance polling.
  - All the states of the interface are set to **Not Polled.**
  - The Status of the interface is set to **No Status**.
  - Traps related to the interface (for example, LinkUp or LinkDown), will not be stored.

- **IPv4 / IPv6 Addresses: Direct Management Mode**

  For addresses, setting the Direct Management Mode to **Not Managed** or **Out of Service** has the following effects:
  - No incidents are generated for the address.
  - The State of the address is set to **Not Polled**.
  - The address is excluded from fault and performance polling.
  - Traps related to the address are not stored.

- **Chassis: Direct Management Mode**

  For Chassis, setting the Direct Management Mode to **Not Managed** or **Out of Service** has the following effects:
  - No incidents are generated for the chassis.
  - The State of the object is set to **Not Polled**.
  - The chassis is excluded from fault and performance polling.
  - The status of the chassis is set to **No Status**.
  - Traps related to the chassis are not stored.

- **Cards: Direct Management Mode**

  For Cards, setting the Direct Management Mode to **Not Managed** or **Out of Service** has the following effects:

- No incidents are generated for the card.
- The State of the object is set to **Not Polled**.
- The card is excluded from fault and performance polling.
- The status of the card is set to **No Status**.
- Traps related to the card are not stored.

- **Node Sensor and Physical Sensor: Inherited Management Mode**

  For Node Sensor or Physical Sensor, setting the Direct Management Mode to **Not Managed** or **Out of Service** has the following effects:
  - No incidents are generated for the Node Sensor and Physical Sensor.
  - The State of the object is set to **Not Polled**.
  - The Node Sensor and Physical Sensor is excluded from fault and performance polling.
  - The status of the node sensor or physical sensor is set to **No Status**.
  - Traps related to the Node Sensor and Physical Sensor are not stored.

NNMi provides the Management Mode workspace so that you can quickly view lists of all nodes, interfaces, IP address, chassis, card, node sensor, or physical sensor that NNMi is not currently discovering or monitoring. For information about these views:

To change the Management Mode back to **Managed**, use the **Actions** → **Management Mode** → **Managed**.

Tip: Some objects have child objects (for example, nodes contain interfaces, and interfaces can contain IP addresses). To change the Management Mode back to **Managed** or **Inherited** for the selected object and all associated child objects, use the **Actions** → **Management Mode** → **Managed (Reset All)**.

Related Topics

"How NNMi Users Change a Management Mode" on the next page

"How NNMi Assigns the Management Mode to an Object" below

"Stop or Start Managing an Object" on page 587

How NNMi Assigns the Management Mode to an Object

NNMi discovers nodes according to current settings for Communication Configuration and Monitoring Configuration.

NNMi administrators and Level 2 Operators can fine tune NNMi results: "How NNMi Users Change a Management Mode" on the next page.

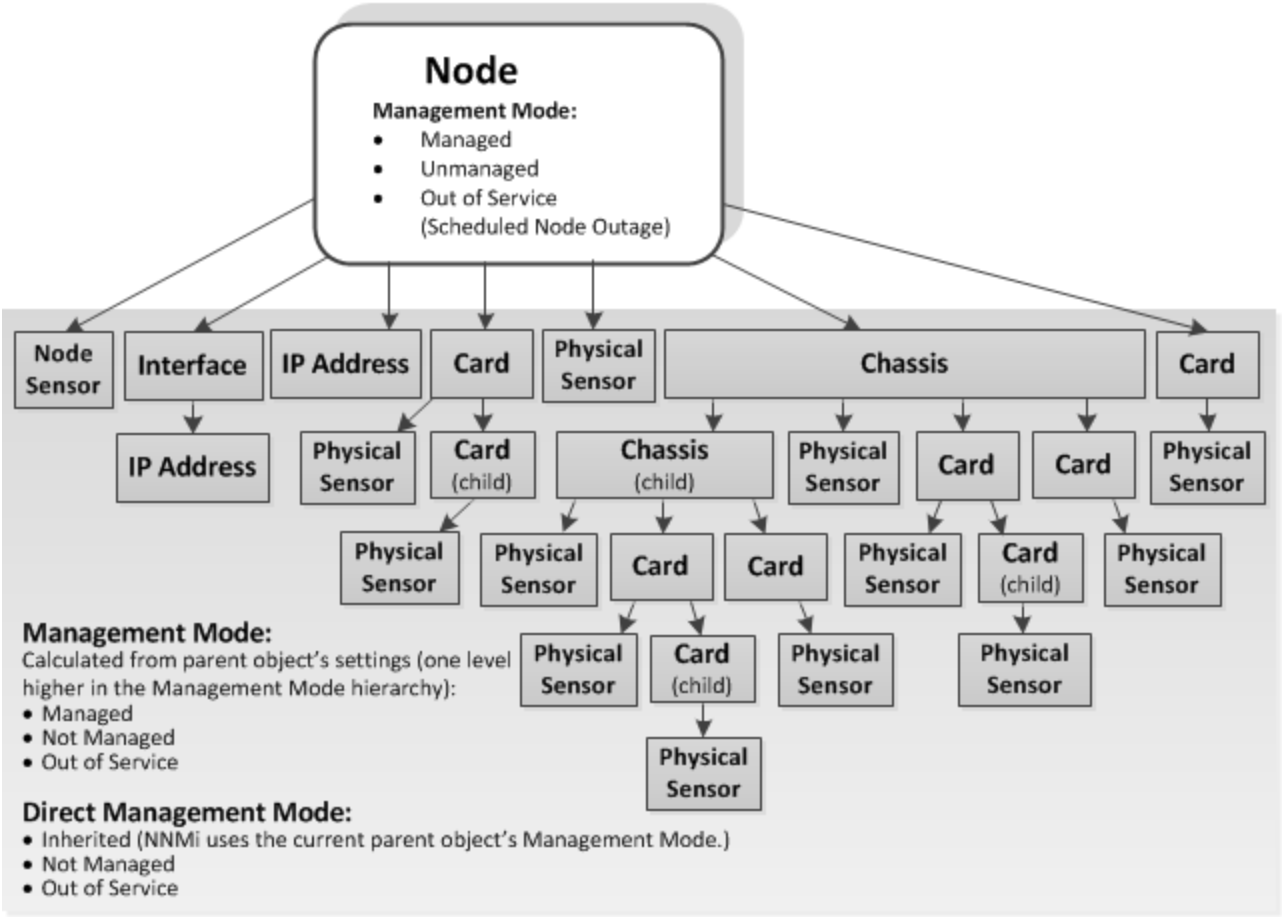
NNMi then calculates each object's Management Mode based on the cumulative settings of all the associated objects higher in the Node's object hierarchy.

For example, NNMi uses the following strategy to determine the Management Mode value for an IP address:

- Direct Management Mode of the IP address (if other than Inherited)
- Direct Management Mode of any associated interface (if other than Inherited)
- Node Management Mode of the parent node

The following illustration show the possibilities for the influence of Management Mode settings.

Hierarchy of Management Mode Settings



How NNMi Users Change a Management Mode

Caution: (*NNMi Advanced - Global Network Management feature*) If your NNMi console is a Global Manager and the selected object is being managed by a Regional Manager (another NNMi management server in your network environment), you cannot change the Management Mode setting unless you log on to the Regional Manager (NNMi management server).

NNMi administrators and Level 2 Operators can change objects management mode.

First review this information: "Understand the Effects of Setting the Management Mode to Not Managed or Out of Service" on page 589.

There are three methods of fine-tuning the NNMi management calculations:

1. Open the object's form, do one of the following, and then select **File** → **Save and Close**:
   - Use the drop-down menu to choose a setting:
     - Node form's **Node Management Mode** drop-down.
     - Interface, IP address, chassis, card, node sensor, or physical sensor form's **Direct Management Mode** drop-down.

       Note: If you are changing the Direct Management Mode, NNMi also updates that object's Management Mode value after you reopen or refresh the form.

   - Use **Actions** → **Management Mode** and choose an available setting for that object.
2. Open a view that contains the objects and do the following:
   a. Select the objects of interest:
      - In a table view, select the row or `Ctrl-click` the rows representing the object information.

        Tip: Right-click a column heading and select **Filter** to quickly generate a list of all nodes with some common aspect.

      - In a map view, single-click the object icon or `Ctrl-click` multiple object icons.

   b. Right-click within the selected block of objects, select **Actions** → **Management Mode**, and choose an available setting for management mode.
3. Use the nnmmanagementmode.ovpl command line tool.

Tip: The next time NNMi polls those devices, the management mode state changes.

Related Topics:

"How NNMi Assigns the Management Mode to an Object" on page 591

"Viewing Lists of the Unmanaged Objects in Your Network" on page 581

Chapter 14: 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**.
2. Navigate to the **State Poller** tab.

   NNMi displays the status of the State Poller, including details about collections, queues, and currently managed objects. For more information, see System Information: State Poller tab.
3. Navigate to the **Custom Poller** tab.

   NNMi displays the status of the Custom Poller, including details about collections, queues, and currently managed objects. For more information, see System Information: State Poller tab and System Information: Custom Poller tab.

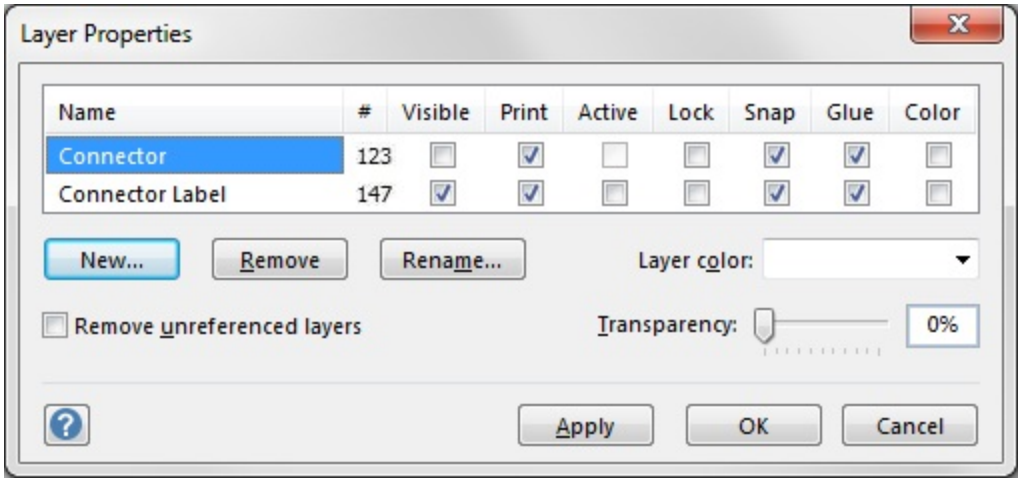
Hide Connections or Connection Labels from an Exported Visio Diagram

Requires HPE Network Node Manager iSPI Network Engineering Toolset Software (NNM iSPI NET) -- click here for more information.

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 **Home** → **Layers** → **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" on page 412

"View the Details for a Map Object on an Exported Visio Diagram" on page 414

"Print an Exported Visio Diagram" on page 414

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.

Autonomous System
An Autonomous System (AS) is a collection of connected Internet Protocol (IP) routing prefixes that present a common, clearly defined Border Gateway Protocol (BPG) routing policy to the Internet by having an officially registered Autonomous System Number (ASN).

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 desination.

CRC
Cyclic Redundancy Check

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 variable when it is evaluated against a node. The first time a MIB variable 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

hypervisor
The virtual machine manager in charge of delegating various aspects from a pool of resources to become virtual devices. The delegations might be static or dynamic, depending on the manufacture's implementation. The type of virtual machines being generated depends on the manufacturer's implementation.

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

J

Jython
Jython is a programming language (successor of JPython) uses Java class, instead of Python modules.

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).

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

MIB file
Management Information Base files are the basic building block of SNMP communication protocol. SNMP Agents are configured to respond to requests defined by a group of supported MIB files.

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.

NIC
Network Interface Controller

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 more limited access privileges than Level 2 Operators), and NNMi Guest Users

Node
A physical or virtual collection of network interfaces that NNMi can pragmatically associate together.

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 desination. 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

SNMP
Simple Network Management Protocol

SNMP Agent
Simple Network Management Protocol (SNMP) is an Internet-standard protocol used to manage devices on IP networks. The SNMP Agent uses this protocol to report information to authorized management programs.

SOAP
Simple Object Access Protocol

Split Link Aggregation
Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

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".

USM
User-based Security Model

UUID
Universally Unique Object Identifier, which is unique across all databases.

V

virtual machine
A device that utilizes components from multiple physical devices. Depending on the manufacture's implementation, the virtual machine may be static or dynamic.

VMware
VMware ESX and VMware ESXi software uses SOAP protocol to implement bare-metal hypervisors.

VRRP
Virtual Router Redundancy Protocol

W

WAN Cloud
Layer 3 connectivity between your network and any MPLS networks.

Web Agent
The Web Agent represents a management service running on a device and contains the settings NNMi uses to communicate with the device.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Online Help: Help for Operators (Network Node Manager i Software 10.20)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to network-management-doc-feedback@hpe.com.

We appreciate your feedback!