

HP Network Node Manager iSPI Performance for Quality Assurance

Software Version: 10.10
Windows® and Linux® operating systems

Online Help

Document Release Date: November 2015
Software Release Date: November 2015



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Oracle Technology — Notice of Restricted Rights

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

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

Copyright Notice

© Copyright 2011 - 2015 Hewlett-Packard Development Company, L.P.

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/>).

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

Accessing the Quality Assurance Workspace	10
Part I: Help for Operators	12
QA Probes	12
Chapter 1: Accessing QA Probe Details	14
Viewing Probe Status	19
QA Probe Form: Left Panel	19
Probes Form: Right Panel	21
Probe State	22
Threshold State	22
Baseline State	25
Status	25
Conclusions	26
Incidents	28
Registration	32
HTTP(S)	32
Identifying Probes with Critical Status	34
Identifying Probes with Threshold Exceptions	36
Identifying Probes with Baseline Exceptions	42
Supported QA Probe Statuses	45
Administrative State	47
Operational State	48
Chapter 2: Measuring Ping Latency	50
Accessing the Ping Latency Pairs Inventory View	50
Viewing Ping Latency Pair Details	52
Valid Ping Latency Pair Statuses	53
Chapter 3: Accessing QoS Details	56
Viewing QoS Interface Details	56
In Policy	58
Out Policy	58
Threshold State	59
QoS Interfaces Form: Incidents Tab	61
QoS In or Out Policy	62
Analysis Pane	62
Viewing QoS Policy Details	64
Interfaces	65
Traffic Classes	66
QoS Policy Hierarchy	67
Viewing QoS Actions Details	69
Interfaces	71
QoS Policies	72

Threshold States	73
Quality of Service (QoS) Actions	74
QoS Class Map Form	75
Identifying QoS Interfaces with Threshold Exceptions	75
Accessing the QoS Actions Threshold Exceptions Inventory View	78
Chapter 4: Accessing QA Group Details	81
Viewing QA Group Details	81
Probes	82
Critical Probes	84
Probes with Threshold Exceptions	85
Probes with Baseline Exceptions	89
Registration	91
QoS Interfaces	92
QoS Actions	92
QoS Interfaces with Threshold Exceptions	93
QoS Actions with Threshold Exceptions	95
Ping Latency Pairs	97
Analysis Pane	98
Viewing QA Probes Using Command Line Utilities	102
Saving QA Probes Using Command Line Utilities	103
Chapter 5: Monitoring Using Maps	105
Using Site Map	106
Launching the Site Map	107
Using Node Response View	111
Launching the Node Response View	112
Using Global Node Response View	115
Launching the Global Node Response View	116
Using QoS Maps	119
QA Group QoS Map	119
QoS Neighbor Map	121
Chapter 6: Monitoring Using Graphs	124
Launching Real Time Line Graphs	124
Chapter 7: Monitoring Using Reports	128
Launching Source Interface Reports	128
Launching Application Health Reports	130
Chapter 8: Monitoring Using Dashboard View	132
Chapter 9: Interpreting Incidents	134
QoS Incident Types Supported by the NNM iSPI Performance for QA	134
Baseline Incidents	135
Threshold Incidents	136
Correlated Incidents	137
Chapter 10: Analyzing the Root Cause of QA Probe Failure	138
Causes for QA Probe Failure Between Nodes	138
Causes for QA Probe Failure Between Sites	139
Part II: Help for Administrators	142

Chapter 1: About the Configuration Console	143
Launching the Quality Assurance Configuration Console	143
Enabling Single Sign-On	148
Chapter 2: About Discovery	149
On-Demand Discovery	149
Parameters	149
Chapter 3: Configuring Ping Latency Pairs	151
Contents of the PingPair.conf File	151
Segments of a Pair Definition	152
Configuring Ping Pairs	153
Configuring Default Ping Attributes	154
Chapter 4: Configuring Discovery Filters	156
Configuring File-Based Node Discovery	157
File-Based Node Exclusion	157
File-Based Node Inclusion	157
Configuring Probe Discovery Filters	159
Adding Probe Discovery Filters	159
Editing Probe Discovery Filters	162
Deleting Probe Discovery Filters	165
Exporting Probe Discovery Filters	165
Importing Probe Discovery Filters	166
Applying On-Demand Probe Discovery Filter	167
Usage:	167
Parameters	167
Configuring QoS Discovery Filters	168
Adding QoS Discovery Filters	168
Editing QoS Discovery Filters	171
Deleting QoS Discovery Filters	172
Exporting QoS Discovery Filters	172
Importing QoS Discovery Filters	173
Applying On-Demand QoS Discovery Filter	174
Usage:	174
Parameters	174
Troubleshooting Discovery Filter Configuration Error Messages	175
Chapter 5: Configuring Sites	178
Launching the Site Configuration Form	179
Adding Sites	180
Editing Sites	185
Deleting Sites	189
Viewing Sites	190
Exporting Sites	190
Importing Sites	191
Associating Probes with Sites	192
Cloning (Copying) Site Configurations	193
Troubleshooting Site Configuration Error Messages	197
Chapter 6: Configuring QA Groups	200

Adding QA Groups	201
Editing QA Groups	204
Deleting QA Groups	207
Exporting QA Group Configurations	207
Importing QA Group Configurations	208
Operators Used in Defining QA Group Filter	209
Values Used in Defining QA Group Filter	210
Chapter 7: Configuring Thresholds	212
Configuring Probe Thresholds	213
Baseline Monitoring	214
Launching the Configure Threshold Form	215
Adding Threshold Settings	217
Editing Threshold Settings	220
Adding Baseline Settings	224
Editing Baseline Settings	226
Deleting Thresholds	228
Troubleshooting Threshold Configuration Error Messages	230
Viewing Probe-Specific Thresholds	232
Configuring Probe Thresholds for QA Groups	234
Adding QA Group Threshold Configuration	235
Adding QA Group for QA Probe Threshold Setting	236
Creating QA Group Baseline Threshold Settings	240
Editing QA Group Threshold Settings	242
Editing QA Group Threshold Setting	243
Editing QA Group Baseline Threshold Settings	246
Editing QA Group Baseline Threshold Settings	247
Deleting QA Group Thresholds	249
Deleting QA Group Baseline Thresholds	249
Importing QA Group Thresholds	249
Exporting QA Group Thresholds	250
Configuring Site Thresholds	251
Adding Threshold Configuration	253
Adding Threshold Settings	254
Adding Baseline Settings	258
Editing Threshold Configuration	260
Editing Threshold Settings	262
Editing Baseline Settings	266
Deleting Thresholds	268
Exporting Thresholds	269
Importing Thresholds	270
Configuring QoS Thresholds	270
Adding QoS Threshold Configuration	272
Adding QoS Threshold Settings	274
Editing QoS Threshold Configuration	276
Editing QoS Threshold Settings	277
Deleting QoS Thresholds	280

Importing QoS Thresholds	280
Exporting QoS Thresholds	281
Supported QoS Threshold Configuration Metrics	281
Configuring QoS Thresholds for QA Groups	284
Adding QoS Threshold Configuration to QA Groups	285
Adding QoS Threshold Settings to QA Groups	286
Editing QoS Threshold Configuration of QA Groups	288
Editing QoS Threshold Settings of QA Groups	289
Deleting QoS Threshold Settings of QA Groups	291
Importing QoS Thresholds of QA Groups	292
Exporting QoS Thresholds of QA Groups	292
Configuring Ping Latency Pair Thresholds	293
Adding Ping Latency Pair Thresholds	294
Adding Threshold Settings	294
Adding Threshold Settings	295
Edit an Existing Ping Pair Threshold	297
Exporting Ping Latency Pair Thresholds	297
Importing the Ping Latency Pair Threshold Configurations	298
Supported Threshold Configuration Metrics	299
Chapter 8: Configuring Global Network Management	302
Launching the Global Network Management Configuration Form	302
Creating Regional Managers	303
Editing Regional Managers	304
Deleting Regional Managers	305
Adding Regional Manager Connections	305
Modifying Regional Manager Connections	307
Deleting Regional Manager Connections	308
Troubleshooting Global Network Management Configuration Error Messages	308
Chapter 9: Configuring Polling	311
Chapter 10: Managing QA Probes	313
Viewing Pre-configured QA Probes Available	313
Creating QA Probe Templates	315
Using QA Probe Templates	319
Viewing Probe Template Inventory	324
Deploying QA Probes	327
Viewing QA Probe List	327
Viewing QA Probe Deployment Status	329
Maintaining QA Probes	331
Viewing the List of Probes	331
Viewing Probes with Enabled Status	332
Viewing Probes with Disabled Status	333
Viewing Deleted Probes	334
Managing QA Probes using Command Line Utility	335
Usage	335
Parameters	336
Batch Upload of QA Probes	337

- Managing iRA QA Probes 337
 - Creating iRA QA Probe Templates 337
 - Using iRA QA Probe Templates 341
 - Viewing iRA QA Probe Deployment Status 346
 - Viewing iRA Pre-configured QA Probes Available 348
- Use Cases 350
 - Threshold Configuration 350
 - Summary 350
 - Actors 350
 - Pre Condition 350
 - Configure Threshold 351
 - Assumptions 351
 - Initialization 351
 - Threshold Configuration Process 351
 - Process Termination 352
 - Exceptions 353
 - Post Conditions 353
 - GUIs Referenced 353
 - System Interface 353
- Glossary 354

Accessing the Quality Assurance Workspace

After you install NNM iSPI Performance for QA, a new workspace for Quality Assurance gets added to your NNMi console.

The Quality Assurance workspace displays all the QA probes discovered in the network.

You can launch the detailed information on a selected QA probe using this workspace.

To launch the Quality Assurance workspace:

1. Log on to NNMi console using your user name and password.

User roles determine access to the NNMi console workspaces, forms, and actions. NNMi provides the following roles. It is not possible to create additional roles or change the names of the roles provided by NNMi:

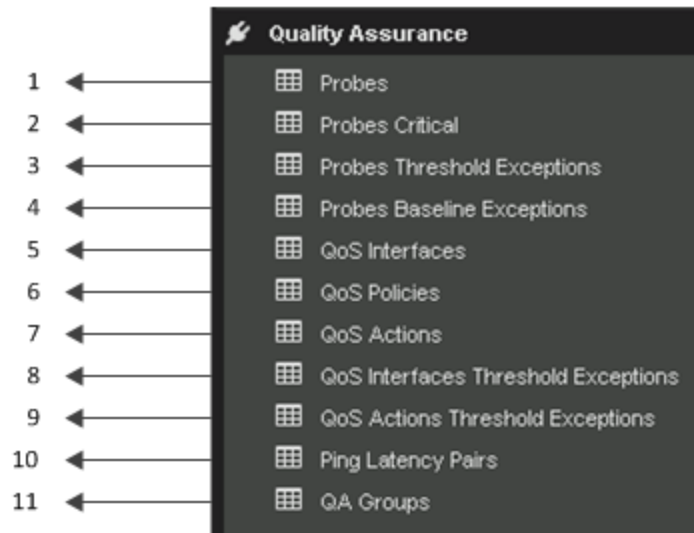
- Administrator
- Operator Level 2
- Operator Level 1
- Guest

You should not use the System role or Web Service Client role. NNMi provides the System role for accessing NNMi the first time during installation and for command line access. NNMi provides a special Web Service Client role to provide access for software that is integrated with NNMi.

See *Set Up Command Line Access in HP Network Node Manager i Software Online Help* for more information

2. Click **Quality Assurance** in the Workspaces panel. The Quality Assurance tab expands, displaying

the various options as shown in the figure below:



Legend	Task
1	Accessing the QA Probes Inventory View
2	Accessing the Critical QA Probes Inventory View
3	Accessing the Probes Threshold Exceptions Inventory View
4	Accessing the Probes Baseline Exceptions Inventory View
5	Accessing the QoS Interfaces Inventory View
6	Accessing the QoS Policies Inventory View
7	Accessing the QoS Actions Inventory View
8	Accessing the QoS Interfaces Threshold Exceptions Inventory View
9	Accessing the QoS Actions Threshold Exceptions Inventory View
10	Accessing Ping Latency Pairs Inventory View
11	Accessing the QA Groups Inventory View

Part I: Help for Operators

NNM iSPI Performance for QA enables you to do the following:

- View the performance of each node in your network and the connectivity between multiple nodes.
- View the performance of each site in your network and the connectivity between multiple sites.
- Discover the QA probes configured in the nodes managed by NNMi.
- Monitor the network performance and view the threshold state of the metric in the NNMi console.
- Analyze the outcome of each QA probe and generate reports up to a maximum period of 13 months.
- Identify the QA probes that violated the threshold for any metric.
- Discover, list, and monitor the QoS interfaces and policies. You can also analyze the mapping between these policies, classes and QoS interfaces available in the network and the QoS policies and actions applied on the QoS interfaces.
- Discover, list, and monitor the ping pair nodes configured on the network.
- View the QA probes or QoS elements based on the QA Groups configured using NNM iSPI Performance for QA.

QA Probes

NNM iSPI Performance for QA does not poll the QA probes for the nodes that have any of the following management modes:

- Not Managed: Indicates that the node is not managed on purpose.
- Out of Service: Indicates that a node is unavailable because it is out of service.

NNM iSPI Performance for QA monitors the network performance with the following metrics:

- Round Trip Time (RTT)
- Jitter
- Packet Loss (Can be from source to destination, destination to source, or two way.)
- Mean Opinion Score (MOS)

For information on metrics, see the topic *NNM iSPI Performance for QA Metrics* in the *NNM iSPI Performance for QA Reports Online Help*.

NNM iSPI Performance for QA discovers the following types of QA probes:

- DNS
- HTTP and HTTPS
- ICMP Echo
- ICMP Jitter
- Oracle
- TCP Connect

- UDP Echo
- UDP
- VoIP
- DHCP

See the *NNM iSPI Performance for QA Support Matrix* for a list of devices on which the NNM iSPI Performance for QA can discover and monitor probes. The Support Matrix also provides information about supported metrics on each device type.

NNM iSPI Performance for QA supports the multi-tenant architecture of NNMi. The security group and tenants configured in NNMi is also applicable for the QA probes in NNM iSPI Performance for QA. See the topic *Configuring Security* in the *NNMi Online Help* for more information on Tenants and Security Groups.

To perform a basic monitoring of the quality of your network performance, follow the steps as discussed below:

Log on to the NNMi console with the operator (level 1 or 2) or guest credentials. After you log on to the NNMi console, you can view the NNM iSPI Performance for QA workspace.

You can access the inventory view to monitor the status and necessary details for the preconfigured QA probes in every device in your network.

NNM iSPI Performance for QA - For Juniper Devices

The probe types on Juniper devices, when discovered by NNM iSPI Performance for QA, are interpreted differently. The following table lists the probe types on the device and their interpretation by NNM iSPI Performance for QA:

Note: The table below is for SRX and MX series of Juniper devices only.

Probe Type on Device	Hardware Timestamp is Enabled	Probe Type in NNM iSPI Performance for QA
icmp-ping/ icmp-ping-timestamp	No	ICMP Echo
icmp-ping/ icmp-ping-timestamp	Yes	ICMP Jitter
udp-ping/ udp-ping-timestamp	No	UDP Echo
udp-ping/ udp-ping-timestamp	Yes	UDP

If hardware timestamp is changed for a probe between two discovery cycles, the probe type also changes accordingly. For example, an udp-ping-timestamp probe with hardware timestamp enabled will be discovered by NNM iSPI Performance for QA as UDP probe. However, if hardware timestamp is disabled later, it will be rediscovered as an UDP Echo probe in the next discovery cycle.

Chapter 1: Accessing QA Probe Details

The QA Probes view displays all the QA probes configured in the [network elements](#)¹. The QA probes are discovered by the NNMi polling process.

To launch the QA Probes view:

1. Log on to NNMi console using your user name and password.
2. Click the **Quality Assurance** workspace. The Quality Assurance tab expands to display the views.
3. Click the **QA Probes** view. The view displays all the QA probes discovered in your network along with some key attributes for each QA probe.
By default, this information is refreshed every 300 seconds, or 5 minutes.

The NNM iSPI Performance for QA supports Multi-Tenancy architecture configured in NNMi. The security group defined for a node in NNMi is also applicable for the probes of the node in NNM iSPI Performance for QA. This implies that all QA probes cannot be viewed by all users. For example, if a user has access to a set of nodes, the user can view only the QA probes configured on those nodes.









To manage large number of QA probes, use the **QA Groups** list to filter the QA probes based on various QA groups. As you type, the auto-complete feature lists the matching QA Groups. You can select a QA Group name from the list.

You can also perform a few other actions on probes by following the steps given below:




1. Right-click a probe and select **Quality Assurance** from the sub-menu.
2. Choose an option from the sub-menu to perform an action you want on the probe.

Key Attributes of the QA Probes View



















The QA Probes view displays the following key attributes for each QA probe:

Attribute Name	Description
Status	<p>The status of the QA probe. NNM iSPI Performance for QA calculates the status based on the polling status of the nodes and the threshold states. A QA probe can have one of the following statuses :</p> <ul style="list-style-type: none">•  Normal•  Warning•  Major•  Critical•  Unknown•  Disabled•  Not Polled•  No Status

¹Some examples of network elements are routers and switches.

Attribute Name	Description
	For more information about the probe status, see the topic "Supported QA Probe Statuses " on page 45.
Name	The name of the discovered QA probe configured on the network device.
Owner	The name of the discovered QA probe's owner.
Service	<p>The type of the discovered QA probe.</p> <p>Some of the QA probe types that the NNM iSPI Performance for QA recognizes are:</p> <ul style="list-style-type: none"> • UDP Echo • ICMP Echo • UDP • TCP Connect • VoIP • HTTP • DNS • DHCP • Oracle • HTTPS
Device Model	The device model name (as discovered by NNMi) of the probe's source node.
Source	The source device on which the probe is configured.
Destination	The destination device on which the probe is configured.
Source Site ¹	The source site to which the configured probe is associated.
Destination Site	The destination site to which the configured probe is associated.
RTT	<p>The round-trip time used by the selected QA probe.</p> <p>Displays one of the following threshold states for the metric:</p> <ul style="list-style-type: none">  High  Nominal  Low

¹A logical organization of networking devices. In the scope of enterprise networks, a site can be a logical grouping of networking devices generally situated in similar geographic location. The location can include a floor, building or an entire branch office or several branch offices which connect to head quarters or another branch office via WAN/MAN. Each site is uniquely identified by its name. In case of the service provider networks the Virtual Routing and Forwarding (VRF) on a Provider Edge (PE) router or a Customer Edge (CE) routers can be defined as a site.








Attribute Name	Description
	 Not Polled  Unavailable  Threshold Not Set  None
Jitter	The delay ¹ variance for a data packet to reach the destination device or site. Displays one of the following threshold states for the metric:  High  Nominal  Low  Not Polled  Unavailable  Threshold Not Set  None
PL (Packet Loss)	The percentage of packets that failed to arrive at the destination. Displays one of the following threshold states for the metric:  High  Nominal  Low  Not Polled  Unavailable  Threshold Not Set  None
Manager	Specifies whether the NNMi management server is Local or specifies the name of the Regional Manager.
Tenant	Specifies the NNMi tenant selected for the QA probe.

The RTT, Jitter, and PL columns display the most recent network performance states. Apart from this, MOS metric is also considered for change in the network performance state.

The following table describes the threshold state or network performance state values:

¹The time taken for a packet to travel from the sender network element to the receiver network element.

Threshold States

State	Description
 High	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and this high value persists for the specified High Duration within the High Duration Window.</p>
 Nominal	<p>Indicates that the measured value of the metric is within the normal healthy range.</p>
 Low	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is below the configured Low Value for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is below the configured Low Value and this low value persists for the specified Low Duration within the Low Duration Window.</p> <p>Typically, this threshold state is applicable for metrics such as Mean Opinion Score (MOS).</p>
 Not Polled	<p>Indicates that the metric is intentionally not polled.</p> <p>Some of the possible reasons are:</p> <ul style="list-style-type: none"> • The parent Node or Interface is set to Not Managed or Out of Service. • The metric is not supported for the particular entity. <p>For example, for an ICMP probe, Jitter and Packet Loss metrics are not supported and so the threshold states for these metrics are displayed as "Not Polled".</p>
 Unavailable	<p>Unable to compute the metric, or the computed value is outside the valid range.</p>
 Threshold Not Set	<p>Indicates that the threshold is not set for the metric.</p>
 None	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero and this zero value persists for the specified duration within the High or Low Duration Window (depending on the metric).</p>

Note: If you launch the Status Poll command from NNMI, it also triggers a corresponding status poll for NNM iSPI Performance for QA.

Analysis Pane

To view the Analysis pane, click a QA probe in the QA Probes View. The Analysis pane of the selected QA Probe appears.

In the **Analysis** pane, you can view the summary, Threshold State, Baseline State, Latest Polled Values, and Performance panels.

The **Threshold State** panel displays whether the threshold is configured for the selected probe or not. It also indicates whether the threshold is configured for a site or a probe. If a threshold is configured, you can view the summary of the threshold configuration details. The configured threshold value and rearm value are displayed in either milliseconds or microseconds based on the probe configuration. The Threshold State pane enables you to check the configured values and the threshold violations, if any.

If the threshold is not configured, you can use the **Configure Threshold** link provided in this pane to configure the threshold.

The **Baseline State** panel displays whether Baseline Monitoring is configured for the selected probe or not. If baseline monitoring is configured, you can view the metric, baseline state, upper norm deviation, and lower norm deviation.







The **Latest Polled Values** panel displays the last five polled values for the relevant metrics, which may be RTT (ms or μ s), two-way jitter (ms or μ s), two-way packet loss, and MOS metric. You can also view the last polled time. If the last polled time is not available, it displays the message—Polling Not Complete.

The **Performance** panel enables you to analyze the performance faults for the selected probe, in the form of graphs. The graph shows the following information:

- RTT value of the selected probe
- Reachability of the selected probe

You can easily monitor and analyze the performance of the probe, from the color of the status. Whenever any problem arises, you can view the status in the **Performance** panel. The status of the probe enables you to easily determine the root cause of the fault.

The following table indicates the status information:

Probe Status	Color in the graph
Normal	 Normal
High, Low	 Major
Critical	 Critical
No Status	 No Status
Unavailable, Unknown	 Unknown
Not Polled, Threshold not set, Not defined	 Disabled

Viewing Probe Status

The QA Probe Form displays the details for the selected QA probe and the configurations associated with it.








QA Probe Form: Left Panel

The left panel of the QA Probe form displays the following:

QA Probe Details

This section displays the following:

Basic Attributes: QA Probe Details

Attribute	Description
Status	<p>Status of the QA probe.</p> <p>A QA probe can have one of the following statuses:</p> <ul style="list-style-type: none"> No Status Normal Disabled Unknown Warning Major Critical <p>For more information about QA probe status, see "Supported QA Probe Statuses" on page 45.</p>
Name	<p>Name of the selected QA probe.</p> <p>For QA probes, the QA probe name is derived from the 'TAG' field of the QA probe definition.</p> <p>If the tag field is not present, the QA probe name is derived by appending the source node name, the target IP address, and the admin index.</p> <p>For RFC QA probes, the name is derived from the RFC MIB.</p> <p>The QA probe names cannot be blank.</p>
Owner	<p>Name of the QA probe owner.</p>
Service	<p>Type of the QA probe.</p> <p>Possible service types are:</p> <ul style="list-style-type: none">UDP Echo




Basic Attributes: QA Probe Details, continued

Attribute	Description
	<ul style="list-style-type: none"> • ICMP Echo • UDP • TCP Connect • VoIP • HTTP • DNS • HTTPS • Oracle • DHCP
Device Model	The device model name (as discovered by NNMi) of the probe's source node.
Admin Index	The unique index ID given for each QA probe. Available only for QA probes.
Manager	Specifies whether the NNMi management server is Local or not. The name of the Regional Manager is displayed if the NNMi management server is not local.
One Way HW Time Stamp Enabled	Specifies whether the one way hardware time stamp is enabled or not for the QA probe.

Source/Destination Info

This section displays the following:

Basic Attributes: Source/Destination Info

Attribute	Description
Source	<p>Name of the starting device from which the QA probe is configured.</p> <p>Click  and select  Show Analysis or  Open to display the Node Form. The Node: <Node Name> form opens. Select the QA Probes tab to display the QA probes initiated from this node.</p>
Source IP Address	IP address of the starting device from which the QA probe is configured.
Source Interface	Interface name to which the QA probe is configured. For information on configuring source interfaces, see Configuring Source Interface for a QA Probe .
Source Site	Name of the site where the source device resides.
Source Port	Port number of the starting device from which the QA probe is configured.
Destination	Name of the end point on which the QA probe is configured.

Basic Attributes: Source/Destination Info, continued

Attribute	Description
Destination IP Address	IP address of the device at the end point on which the QA probe is configured.
Destination Site	Name of the site where the destination device resides.
Destination Port	Port number of the device at the end point on which the QA probe is configured.
Measurement Precision	Whether the QA probe retrieves the network performance in microseconds or in milliseconds.
Timeout	Maximum time the source node waits for a response from the destination node before stopping the request.
Frequency	Frequency of the QA probe in seconds.
TOS	Type of Service specified in an IP packet header that indicates the service level required for the packet.
VRF	Virtual Routing and Forwarding (VRFs) tables defined on the source node. This field is populated only if the test is configured with VRF(s).
Discovery State	Discovered state of the source node. Possible values are as follows: Completed - All the analysis are completed and the QA probes are discovered. In Progress - The discovery process is still gathering network information or the QA probe data.
Last Discovery Completed	Date, time, and time zone of the last discovery.
Management Mode	Whether the source node is managed or not. Possible states are as follows: <ul style="list-style-type: none"> • Managed: Indicates that the node is managed. • Not Managed: Indicates that the node is not managed on purpose. • Out of Service: Indicates that a node is unavailable because it is out of service.

Probes Form: Right Panel

The right panel of the QA Probes form displays information about the selected QA probe. The panel consists of the following tabs:

- [State](#)
- [Threshold State](#)
- [Baseline State](#)
- [Status](#)

- [Conclusions](#)
- [Incidents](#)
- [Registration](#)
- [HTTP\(S\) Configuration](#)

Analysis Pane

The **Analysis** pane enables you to view the Summary, Threshold State, and Latest Polled Values panels.

The **Threshold State** panel displays whether the threshold is configured for the selected probe or not. It also indicates whether the threshold is configured for a site or a probe. If a threshold is configured, you can view the summary of the threshold configuration details. The configured threshold value and rearm value are displayed in either milliseconds or microseconds based on the probe configuration. The Threshold State pane enables you to check the configured values and the threshold violations, if any.

If the threshold is not configured, you can use the **Configure Threshold** link provided in this pane to configure the threshold.

The **Latest Polled Values** panel displays the last five polled values for the relevant metrics, which may be RTT, two-way jitter, or two-way packet loss metric. If the last polled time is not available, it displays the message "Polling Not Complete".

Probe State

The **State** tab in the QA Probes Form displays information about the last run of the QA probe.

Attributes: State Tab



Attribute	Description
Administrative State	Administrative State condition returned by the QA probe. The QA probe status is derived from the SNMP polling results for Administrative State , as well as from any conclusions.
Operational State	Operational State condition returned by the QA probe. The QA probe status is derived from the SNMP polling results for Operational State , as well as from any conclusions.
State Last Modified	The date, time, and time zone when the QA probe state was last modified.

Threshold State









The **Threshold State** tab in the QA Probes Form displays a quick summary of the most recent performance of the [network element](#)¹ on which the QA probe runs.

This tab displays only those metrics on which the administrator has configured a threshold.

¹Some examples of network elements are routers and switches.

When the network performance breaches a threshold depending on the count-based, or time-based threshold configuration, the **Status** tab displays the network element status as  Major and the Incident tab displays a  Critical incident raised on the network element.








This tab displays the following details:




Field Name	Description
State	<p>The threshold state of the probe. The valid threshold states are listed below:</p> <ul style="list-style-type: none">  High  Nominal  Low  Not Polled  Unavailable  Threshold Not Set  None <p>For more information about the threshold states, see Threshold States.</p>
Metric Name	The name of the metric.
Type	The type of threshold configured. It can be Count-Based or Time-Based.
Value	This value indicates the high threshold value, measured in milliseconds or microseconds.
Rearm Value	The Rearm Value is used to indicate the end of the threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value, measured in milliseconds or microseconds.
Trigger Count	Indicates after how many consecutive threshold violations NNM iSPI Performance for QA alerts the operator by transitioning the threshold state to  High. This field value appears for Count-based threshold configuration.
Duration	Indicates the minimum duration for which the value must persist in a high value range for the threshold state to change to High. This field value appears for Time-based threshold configuration.
Duration Window	Indicates the duration of the window within which the high duration criteria must be met. This field value appears for Time-based threshold violations.

Threshold States

The following table describes the threshold states:

Threshold States








State	Description
 High	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and this high value persists for the specified High Duration within the High Duration Window.</p>
 Nominal	Indicates that the measured value of the metric is within the normal healthy range.
 Low	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is below the configured Low Value for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is below the configured Low Value and this low value persists for the specified Low Duration within the Low Duration Window.</p> <p>Typically, this threshold state is applicable for metrics such as Mean Opinion Score (MOS).</p>
 Not Polled	<p>Indicates that the metric is intentionally not polled.</p> <p>Some of the possible reasons are:</p> <ul style="list-style-type: none"> • The parent Node or Interface is set to Not Managed or Out of Service. • The metric is not supported for the particular entity. <p>For example, for an ICMP probe, Jitter and Packet Loss metrics are not supported and so the threshold states for these metrics are displayed as "Not Polled".</p>
 Unavailable	Unable to compute the metric, or the computed value is outside the valid range.
 Threshold Not Set	Indicates that the threshold is not set for the metric.
 None	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero and this zero value persists for the specified duration within the High or Low Duration Window (depending on the metric).</p>

- Click  **Open** to view more information about a specific threshold state.
- Click  **Refresh** to refresh the Threshold State table.
- Click  **Show View in New Window** to open the Threshold State table in an independent window.

Baseline State

The **Baseline State** tab in the QA Probes Form displays only those metrics on which the administrator has configured a baseline deviation setting.







The valid baseline states for the QA probes are listed below:

-  Normal Range - The metric is within the normal range of deviation.
-  Abnormal Range - The metric is either above or below the configured normal range of the deviation.
-  Unavailable - The computed value for the metric is not found in HP NNM iSPI Performance for Metrics Software.
-  Unset - No baseline is computed.
-  Not polled - The metric is not polled for baseline deviations.
-  No Policy - No polling policy exists for this metric.
-  Threshold Agent Error - Indicates an error was returned by the state poller when retrieving the data from NPS.




Status

The **Status** tab in the QA Probes Form displays a quick summary of the iSPI object status to better determine and monitor any significant patterns in behavior and activity.

Attribute: Status Tab

Attribute	Description
Status	<p>Overall status for the current QA probe</p> <p>Possible values are:</p> <ul style="list-style-type: none">•  No Status•  Normal•  Disabled•  Unknown•  Warning•  Major






Attribute: Status Tab, continued

Attribute	Description
	<ul style="list-style-type: none"> •  Critical <p>For more information on the QA probe status, see the "Supported QA Probe Statuses " on page 45.</p> <p>In the case of sub-minute polling, the QA probe status refreshes every 2 minutes. The QA probe status gets updated based on the average polling value obtained for the last 2 minutes.</p> <p>For more information about how the current status was determined, see the following topics:</p> <ul style="list-style-type: none"> • "Probe State" on page 22 • "Conclusions " below
Status Last Modified	<p>Current status is calculated and set by Causal Engine.</p> <p>The Time Stamp data displays the time when the status of the QA probe is last updated.</p>
Status History	<p>List of up to the last 30 changes in status for the selected QA probe.</p> <p>This view is useful for obtaining a summary of the QA probe status so that you can better determine any patterns in traffic between the source node or site and the destination node or site.</p> <ul style="list-style-type: none"> • Click  Refresh to refresh the Status History table. • Click  Show View in New Window to open the Status History table in an independent window.



Conclusions

The **Conclusions** tab in the QA Probe Form displays the results of the overall derived status. You can get a quick summary of the status and problem description retrieved by the selected QA probe.

Attribute: Conclusions Tab

Attribute	Description
Status	<p>Status of the conclusion.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> •  No Status •  Normal •  Disabled •  Unknown •  Warning

Attribute: Conclusions Tab, continued

Attribute	Description
	<ul style="list-style-type: none"> •  Major •  Critical <p>For more information on the QA probe status, see the "Supported QA Probe Statuses" on page 45.</p> <p>Status reflects the most serious outstanding conclusion.</p>
Time Stamp	Displays the time when the status of the QA probe was last updated.
Conclusions	<p>Dynamically generated list of summary statuses of the QA probe at points in time that contributed to the current overall status of the selected QA probe.</p> <p>Status is set by the Causal Engine. This view is useful for obtaining a quick summary of the status and problem description for the QA probe's most current status.</p> <p>Examples of conclusions that might appear together are listed below:</p> <ul style="list-style-type: none"> • TestUp¹ • RttThresholdStateHigh • TwoWayPktLossThresholdStateHigh <p>Following examples list some of the conclusions caused by Administrative and Operational states:</p> <p>Conclusions caused by Administrative State</p> <p>TestTransient</p> <ul style="list-style-type: none"> • notready • createandwait • createandgo • destroy <p>TestDisabled</p> <ul style="list-style-type: none"> • disabled • Notinservice <p>TestUnknown</p> <p>Caused by an SNMP error.</p> <p>TestUnpolled</p>

¹When both Administrative and Operational states are up.

Attribute: Conclusions Tab, continued

Attribute	Description
	<p>Caused when the QA probe is not polled.</p> <p>Conclusions caused by Operational State</p> <p>TestFailed</p> <ul style="list-style-type: none"> • OperStateTimeout on probe • OperStateDisconnected on probe • OperStateNotConnected on probe • OperStateApplicationSpecific on probe • OperStateDnsServerTimeout on probe • OperStateTcpConnectTimeout on probe • OperStateHttpTransactionTimeout on probe • OperStateDnsQueryError on probe • OperStateHttpError on probe • OperStateError on probe • OperStateDisabled on probe <p>TestError</p> <p>OperStateOther on probe</p> <p>OperStateSequenceError on probe</p> <p>OperStateOverThreashold on probe</p> <p>OperStateBusy on probe</p> <p>OperStateVerifyError on probe</p> <p>OperStateDropped on probe</p> <p>For information about how conclusions are based on the QA probe states, see "Probe State" on page 22.</p>

Incidents

The **Incidents** tab in the QA Probes Form displays a quick summary of the problem description retrieved by the QA probe.

You can view the incidents only if you have the permissions to access the source node.

Attribute: Incidents Tab

Attribute	Description
Incidents Attributes	<p>The attributes listed in the incidents tab are same as the ones available in the NNMI Incidents form.</p> <p>For more information about the Incidents attributes, see the topic <i>NNMI Incidents Form</i> in the <i>Network Node Manager i Software Online help</i>.</p> <p>NNM iSPI Performance for QA generates the following incidents:</p> <p>TwoWayJitterHigh</p> <p>Indicates a high two-way jitter value (which is the average of the following values):</p> <ul style="list-style-type: none"> • Positive jitter from the source to the destination • Negative jitter from the source to the destination • Positive jitter from the destination to the source • Negative jitter from the destination to the source <p>SourceToDestinationPositiveJitterHigh</p> <p>Indicates a high positive jitter from the source to the destination. The jitter value is collected from the MIB. The exact MIB values that are queried may vary based on whether the latest value is polled or cumulative value is polled.</p> <p>DestinationToSourcePositiveJitterHigh</p> <p>Indicates a high positive jitter from the destination to the source. The jitter value is collected from the MIB. The exact MIB values that are queried vary based on whether the latest value is polled or cumulative value is polled.</p> <p>SourceToDestinationNegativeJitterHigh</p> <p>Indicates a high negative jitter from the source to the destination. The jitter value is collected from the MIB. The exact MIB values that are queried vary based on whether the latest value is polled or cumulative value is polled.</p> <p>DestinationToSourceNegativeJitterHigh</p> <p>Indicates a high negative jitter from the destination to the source. The jitter value is collected from the MIB. The exact MIB values that are queried vary based on whether the latest value is polled or cumulative value is polled.</p> <p>TwoWayPacketLossHigh</p> <p>Indicates a high percentage of two-way packet loss. This value is the average of the following values:</p> <ul style="list-style-type: none"> • Packet loss percentage from the source to the destination • Packet loss percentage from the destination to the source <p>SourceToDestinationPacketLossHigh</p> <p>Indicates a high percentage of packet loss from the source to the destination.</p>










Attribute: Incidents Tab, continued

Attribute	Description
	<p>The packet loss percentage is calculated from the ratio of the total number of packets sent to the reported number of packets lost.</p> <p>The exact MIB values that are queried vary based on whether the latest value is polled or cumulative value is polled.</p>
	<p>DestinationToSourcePacketLossHigh</p> <p>Indicates a high percentage of packet loss from the destination to the source.</p> <p>The packet loss percentage is calculated from the ratio of the total number of packets sent to the reported number of packets lost.</p> <p>The exact MIB values that are queried vary based on whether the latest value is polled or cumulative value is polled.</p>
	<p>RoundTripTimeHigh</p> <p>Indicates a high round trip time. The exact MIB values that are queried vary based on whether the latest value is polled or cumulative value is polled.</p>
	<p>MeanOpinionScoreLow</p> <p>Indicates a low mean opinion score. The exact MIB values that are queried vary based on whether the latest value is polled or cumulative value is polled.</p>
	<p>RoundTripTimeAbnormal</p> <p>Indicates that the round trip time is beyond the normal range. This implies that the round trip time is above the configured normal range of the deviation.</p>
	<p>TwoWayPacketLossAbnormal</p> <p>Indicates the two-way packet loss is beyond the normal range. This implies that the two-way packet loss is above the configured normal range of the deviation. This value is the average of the following values:</p> <ul style="list-style-type: none"> • Packet loss percentage from the source to the destination • Packet loss percentage from the destination to the source
	<p>TwoWayJitterAbnormal</p> <p>Indicates that the two-way jitter is beyond the normal range. This implies that the two-way jitter is above the configured normal range of the deviation. The two-way jitter value is the average of the following values:</p> <ul style="list-style-type: none"> • Positive jitter from the source to the destination • Negative jitter from the source to the destination • Positive jitter from the destination to the source • Negative jitter from the destination to the source
	<p>MeanOpinionScoreAbnormal</p>







Attribute: Incidents Tab, continued

Attribute	Description
	Indicates that the Mean Opinion Score is beyond the normal range. This implies that the mean opinion score is either above or below the configured normal range of the deviation.
	<p>TestError</p> <p>This incident indicates that the QA Probe has returned an error.</p>
	<p>TestTransient</p> <p>This incident indicates that the QA Probe is in a transient state.</p>
	<p>TestFailed</p> <p>This incident indicates that the QA Probe has failed to run.</p>
	<p>TestDisabled</p> <p>This incident indicates that the QA Probe is explicitly disabled by the device administrator.</p>

Attributes: Incidents Tab

Attribute	Description
Severity	<p>Severity of the incident calculated by NNMI. Possible values are:</p> <ul style="list-style-type: none"> •  Normal •  Warning •  Minor •  Major •  Critical •  Unknown •  Disabled •  Not Polled •  No Status
Lifecycle State	Identifies where the incident is in the incident lifecycle.
Last Occurrence	<p>Used when suppressing duplicate incidents or specifying an incident rate.</p> <p>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.</p> <p>If there are no duplicate incidents or incidents that have a rate criteria that were met, then this date is same as the First Occurrence Time.</p>

Attributes: Incidents Tab, continued

Attribute	Description
Correlation Nature	This incident's contribution to a root-cause calculation, if any.
Source Node	The Name attribute value of the node associated with the incident. For more information about the node, click the  Lookup icon and select  Show Analysis or  Open to display the Node Form.
Source Object	Name used to indicate the configuration item that is malfunctioning on the source node. For more information about the object, click the  Lookup icon and select  Show Analysis or  Open to display the Node Form.
Message	The incident message defined by NNMI.

The global manager raises incidents for the overall health of the configured QA Probe interfaces on the network based on the threshold states collected from all regional managers.

For detailed information on NNMI incidents, see the *Incident Form* topic in HP Network Node Manager i Software *Help for Operators*.

Registration

The **Registration** tab in the QA Probe Form displays the results of the overall derived status from the database.

Registration

Attribute	Description
Created	The last date and time when any of the QA probes user interface attributes were created.
Status Last Modified	The last date and time when any of the QA Probe user interface attributes were modified.

Object Identifiers

Attribute	Description
ID	The Unique Object Identifier that is unique for probes.
UUID	The Universally Unique Object Identifier that is unique across all databases.

HTTP(S)

The **HTTP(S)** tab displays the retrieved information about the protocol and proxy.

Protocol Details

Attribute	Description
URL	The URL specified while configuring the probe.
User Name	The user name required to access the URL.

Proxy Details

Attribute	Description
Proxy	The host name of the proxy server.
User Name	The user name for the proxy server.
Port	The port number on which the proxy server is configured.

Identifying Probes with Critical Status

The Critical Probes view is used to segregate and display only the QA probes whose status is critical. The critical QA probes view displays the operational state, and administrative state as well. These details and the details in the Conclusions tab of the QA probe enable you to drill-down to the root cause of the problem.

To launch the Critical Probes view:

1. Log on to NNMi console using your user name and password.
2. Click **Quality Assurance** in the Workspaces panel. The Quality Assurance tab expands.
3. Click **Critical Probes**. The QA probes with Critical status that are discovered in your network appear in the content pane along with some key attributes for each QA probe. By default, this information is refreshed every 300 seconds, or 5 minutes.

The NNM iSPI Performance for QA supports Multi-Tenancy architecture configured in NNMi. The security group defined for a node in NNMi is also applicable for the critical probes of the node in NNM iSPI Performance for QA. This implies that all the critical QA probes cannot be viewed by all users. For example, if a user has access to a set of nodes, then that user can view only the critical QA probes configured on those nodes.

You can filter the critical QA probes based on the QA Groups and list only the critical QA probes that belong to a particular QA group. As you type, the auto-complete feature lists the matching QA Groups. You can select a QA Group name from the list.

Key Attributes of the Critical Probes View

The Critical Probes view displays the following key attributes:

Attribute Name	Description
Operational State	Operational State condition returned by the critical QA probe. The QA probe status is derived from the SNMP polling results for Operational State , as well as from any conclusion.
Administrative State	Administrative State condition returned by the critical QA probe. The QA probe status is derived from the SNMP polling results for Administrative State , as well as from any conclusion.
Name	The name of the discovered QA probe configured in the network device.
Owner	The name of the discovered QA probe's owner.
Service	The type of the discovered QA probe.

Attribute Name	Description
Device Model	The device model name (as discovered by NNMi) of the probe's source node.
Source	The source device from which the data packet is sent.
Destination	The network device to which the data packet is sent.
Source Site ¹	The network site from which the data packet is sent.
Destination Site	The network site to which the data packet is sent.
Manager	Specifies whether the NNMi management server is Local or not. The name of the Regional Manager is displayed if the NNMi management server is not local.
Source Tenant	Specifies the NNMi tenant selected for the source network device.

Note: If you launch the Status Poll command from NNMi, it triggers a corresponding status poll for NNM iSPI Performance for QA as well.

Analysis Pane

Select the QA probe by clicking the QA probe in the Critical QA Probes View to view the Analysis pane. The Analysis pane of the selected Critical QA Probe appears below.

In the **Analysis** pane, you can view the summary, Threshold State, and Baseline State panels.

The **Threshold State** panel displays whether the threshold is configured for the selected probe or not. If a threshold is configured, you can view the summary of the threshold configuration details, and you can also view whether the threshold is configured based on site or a probe. The Threshold State panel enables you to check the configured values and the threshold violations, if any.

The **Baseline State** panel displays whether Baseline Monitoring is configured for the selected probe or not. If baseline monitoring is configured, you can view the metric, baseline state, upper norm deviation, and lower norm deviation.

¹A logical organization of networking devices. In the scope of enterprise networks, a site can be a logical grouping of networking devices generally situated in similar geographic location. The location can include a floor, building or an entire branch office or several branch offices which connect to head quarters or another branch office via WAN/MAN. Each site is uniquely identified by its name. In case of the service provider networks the Virtual Routing and Forwarding (VRF) on a Provider Edge (PE) router or a Customer Edge (CE) routers can be defined as a site.

Identifying Probes with Threshold Exceptions

The Probes Threshold Exceptions view displays a set of probes that have violated the threshold for any one or more of the metrics of NNM iSPI Performance for QA. You can view the threshold states of all the metrics to quickly identify the metrics that have breached the threshold level.

The QA Probes view gives a quick overview of the threshold state violations for the metrics such as Jitter, RTT and so on. However, the Probes Threshold Exceptions view is very exhaustive, and displays intricate details of threshold state violations. This view is very useful for segregating the QA probes that have violated the threshold state and for arriving at a conclusion.

To launch the Probes Threshold Exceptions view:




1. Log on to NNMi console using your user name and password.
2. Click **Quality Assurance** in the Workspaces panel. The Quality Assurance tab expands.
3. Click **Probes Threshold Exceptions**. The QA probes that have violated the threshold for Jitter, RTT, Packet Loss and Mean Opinion Score metrics appear in the content pane along with some key attributes for each QA probe.

















By default, this information is refreshed every 300 seconds, or 5 minutes.

The NNM iSPI Performance for QA supports Multi-Tenancy architecture configured in NNMi. The security group defined for a node in NNMi is also applicable for the probes of the node in NNM iSPI Performance for QA. This implies that all threshold violated QA probes cannot be viewed by all users. For example, if a user has access to a set of nodes, the user can view the threshold violated QA probes configured on those nodes only.






















You can filter the QA probes that violated the threshold, based on the various QA groups. As you type, the auto-complete feature lists the matching QA Groups. You can select a QA Group name from the list.






















Key Attributes of the Probes Threshold Exceptions View





Attribute Name	Description
Status	<p>The status of the QA probes. It can be one of the following:</p> <ul style="list-style-type: none">•  Warning•  Major•  Critical <p>NNM iSPI Performance for QA calculates the status based on the polling status of the nodes and the threshold states.</p> <p>For more information about probe status, see "Supported QA Probe Statuses" on page 45.</p>
Name	The name of the discovered QA probe configured in the network device.
Service	The type of the discovered QA probe.
Device Model	The device model name (as discovered by NNMi) of the probe's

Attribute Name	Description
	source node.
Manager	Specifies whether the NNMi management server is local or not. The name of the Regional Manager is displayed if the NNMi management server is not local.
RTT	<p>The round-trip time used by the selected QA probe.</p> <p>Displays one of the following threshold states for the metric:</p> <ul style="list-style-type: none">  High  Nominal  Low  Not Polled  Unavailable  Threshold Not Set  None
Jitter	<p>The delay¹ variance for a data packet to reach the destination device or site.</p> <p>Displays one of the following threshold states for the metric:</p> <ul style="list-style-type: none">  High  Nominal  Low  Not Polled  Unavailable  Threshold Not Set  None
+ve Jitter SD	<p>Indicates the threshold state of the positive jitter from the source to the destination.</p> <p>Displays one of the following threshold states for the metric:</p> <ul style="list-style-type: none">  High  Nominal

¹The time taken for a packet to travel from the sender network element to the receiver network element.





Attribute Name	Description
	<p> Low</p> <p> Not Polled</p> <p> Unavailable</p> <p> Threshold Not Set</p> <p> None</p>
+ve Jitter DS	<p>Indicates the threshold state of the positive jitter from the destination to the source.</p> <p>Displays one of the following threshold states for the metric:</p> <p> High</p> <p> Nominal</p> <p> Low</p> <p> Not Polled</p> <p> Unavailable</p> <p> Threshold Not Set</p> <p> None</p>
-ve Jitter SD	<p>Indicates the threshold state of the negative jitter from the source to the destination.</p> <p>Displays one of the following threshold states for the metric:</p> <p> High</p> <p> Nominal</p> <p> Low</p> <p> Not Polled</p> <p> Unavailable</p> <p> Threshold Not Set</p> <p> None</p>
-ve Jitter DS	<p>Indicates the threshold state of the negative jitter from the destination to the source.</p> <p>Displays one of the following threshold states for the metric:</p> <p> High</p> <p> Nominal</p>

Attribute Name	Description
	<ul style="list-style-type: none">  Low  Not Polled  Unavailable  Threshold Not Set  None
PL (Packet Loss)	<p>The percentage of packets that failed to arrive at the destination.</p> <p>Displays one of the following threshold states for the metric:</p> <ul style="list-style-type: none">  High  Nominal  Low  Not Polled  Unavailable  Threshold Not Set  None
Packet Loss SD	<p>Indicates the threshold state of the percentage of packet loss from the source to the destination.</p> <p>Displays one of the following threshold states for the metric:</p> <ul style="list-style-type: none">  High  Nominal  Low  Not Polled  Unavailable  Threshold Not Set  None
Packet Loss DS	<p>Indicates the threshold state of the percentage of packet loss from the destination to source.</p> <p>Displays one of the following threshold states for the metric:</p> <ul style="list-style-type: none">  High  Nominal




Attribute Name	Description
	 Low  Not Polled  Unavailable  Threshold Not Set
MOS	Indicates the threshold state of Mean Opinion Score (MOS) of the jitter.
Source Tenant	Specifies the NNMi tenant selected for the source network device.

The following table describes the threshold state values:

Threshold States

State	Description
 High	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and this high value persists for the specified High Duration within the High Duration Window.</p>
 Nominal	Indicates that the measured value of the metric is within the normal healthy range.
 Low	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is below the configured Low Value for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is below the configured Low Value and this low value persists for the specified Low Duration within the Low Duration Window.</p> <p>Typically, this threshold state is applicable for metrics such as Mean Opinion Score (MOS).</p>
 Not Polled	<p>Indicates that the metric is intentionally not polled.</p> <p>Some of the possible reasons are:</p> <ul style="list-style-type: none"> • The parent Node or Interface is set to Not Managed or Out of Service. • The metric is not supported for the particular entity. <p>For example, for an ICMP probe, Jitter and Packet Loss metrics are not supported and so the threshold states for these metrics are displayed as "Not Polled".</p>

Threshold States, continued

State	Description
 Unavailable	Unable to compute the metric, or the computed value is outside the valid range.
 Threshold Not Set	Indicates that the threshold is not set for the metric.
 None	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero and this zero value persists for the specified duration within the High or Low Duration Window (depending on the metric).</p>

Note: If you launch the Status Poll command from NNMi, it triggers a corresponding status poll for NNM iSPI Performance for QA as well.

Analysis Pane

Select the QA probe by clicking the QA probe in the Probes Threshold Exceptions View to view the Analysis pane. The Analysis pane of the selected QA Probe appears.

In the **Analysis** pane, you can view the summary, Threshold State, Baseline State, and Latest Polled Values panels.

The **Threshold State** panel displays the summary of the threshold violations. It also displays whether the threshold configuration is based on probe or site.

The **Baseline State** panel displays whether Baseline Monitoring is configured for the selected probe or not. If baseline monitoring is configured, you can view the metric, baseline state, upper norm deviation, and lower norm deviation.

The **Latest Polled Values** panel displays the last five polled values for the relevant metrics, which may be RTT (ms or μ s), two-way jitter (ms or μ s), two-way packet loss, and MOS metric. You can also view the last polled time. If the last polled time is not available, it displays the message—Polling Not Complete.

Identifying Probes with Baseline Exceptions

The Probes Baseline Exceptions view displays the QA probes with the baseline state as Abnormal Range, Unavailable, No Policy, or Not Polled for any one or more of the following metrics:

- RTT
- Two Way Jitter
- Two Way Packet Loss
- MOS

For information about how baseline state is set, see ["Baseline Monitoring" on page 214](#).

This view is very useful to segregate the QA probes with Baseline exceptions and to arrive at a conclusion.

To launch the Probes Baseline Exceptions view:









1. Log on to NNMi console using your user name and password.
2. Click **Quality Assurance** in the Workspaces panel. The Quality Assurance tab expands.
3. Click **Probes Baseline Exceptions**. The QA probes with the baseline state as Abnormal Range, Unavailable, or Not Polled for any one or more of the metrics appear in the content pane along with some key attributes for each QA probe.













By default, this information is refreshed every 300 seconds, or 5 minutes.













The NNM iSPI Performance for QA supports Multi-Tenancy architecture configured in NNMi. This implies that all baseline exception QA probes cannot be viewed by all users. For example, if a user has access to a set of source nodes, then that user can view only the QA probes configured on those source nodes.

You can filter the QA probes with the baseline state as Abnormal Range, Unavailable, No Policy, or Not Polled, based on the various QA groups. As you type, the auto-complete feature lists the matching QA Groups. You can select a QA Group name from the list.

Key Attributes of the Probes Baseline Exceptions View

Attribute Name	Description
Status	Displays the status of the QA probes. It can be one of the following: <ul style="list-style-type: none">•  Normal•  Warning•  Major•  Critical•  Unknown•  Disabled•  Not Polled•  No Status

Attribute Name	Description
	<p>NNM iSPI Performance for QA calculates the status based on the polling status of the nodes and the threshold states. For more information about status, see "Supported QA Probe Statuses " on page 45.</p>
Name	<p>The name of the discovered QA probe configured in the network device.</p>
Service	<p>The type of the discovered QA probe.</p>
Device Model	<p>The device model name (as discovered by NNMi) of the probe's source node.</p>
Manager	<p>Specifies whether the NNMi management server is local or not. The name of the Regional Manager is displayed if the NNMi management server is not local.</p>
RTT	<p>The round-trip time used by the selected QA probe.</p> <p>Displays one of the following baseline states for the metric:</p> <ul style="list-style-type: none"> •  Normal Range - The metric is within the normal range of deviation. •  Abnormal Range - The metric is above the configured normal range of the deviation. •  Unavailable - The computed value for the metric is not found in HP NNM iSPI Performance for Metrics Software. •  Unset - No baseline is computed. •  Not polled - The metric is not polled for baseline deviations. •  No Policy - No polling policy exists for this metric.
Two Way Jitter	<p>Indicates two way jitter. This value is the average of the following values:</p> <ul style="list-style-type: none"> • Positive jitter from the source to the destination • Negative jitter from the source to the destination • Positive jitter from the destination to the source • Negative jitter from the destination to the source <p>Displays one of the following baseline states for the metric:</p> <ul style="list-style-type: none"> •  Normal Range - The metric is within the normal range of deviation. •  Abnormal Range - The metric is either above or below the configured normal range of the deviation. •  Unavailable - The computed value for the metric is not found in HP NNM iSPI Performance for Metrics Software. •  Unset - No baseline is computed. •  Not polled - The metric is not polled for baseline deviations. •  No Policy - No polling policy exists for this metric.

Attribute Name	Description
Two Way Packet Loss	<p>The percentage of packets that failed to arrive from the source to destination and destination to source.</p> <p>Displays one of the following baseline states for the metric:</p> <ul style="list-style-type: none"> •  Normal Range - The metric is within the normal range of deviation. •  Abnormal Range - The metric is either above or below the configured normal range of the deviation. •  Unavailable - The computed value for the metric is not found in HP NNM iSPI Performance for Metrics Software. •  Unset - No baseline is computed. •  Not polled - The metric is not polled for baseline deviations. •  No Policy - No polling policy exists for this metric.
MOS	<p>Indicates the baseline state of Mean Opinion Score (MOS) of the jitter.</p> <p>Displays one of the following baseline states for the metric:</p> <ul style="list-style-type: none"> •  Normal Range - The metric is within the normal range of deviation. •  Abnormal Range - The metric is either above or below the configured normal range of the deviation. •  Unavailable - The computed value for the metric is not found in HP NNM iSPI Performance for Metrics Software. •  Unset - No baseline is computed. •  Not polled - The metric is not polled for baseline deviations. •  No Policy - No polling policy exists for this metric.
Source Tenant	Specifies the NNMi tenant selected for the source network device.







The default polling interval for the HP NNM iSPI Performance for Metrics Software data to detect the exception is 2 minutes.



Analysis Pane

Select the QA probe by clicking the QA probe in the Probes Baseline Exceptions view. The Analysis pane of the selected QA Probe appears. The **Baseline State** panel displays the metric, baseline state, upper norm deviation, and lower norm deviation.

Supported QA Probe Statuses

The system displays one of the following valid QA probe statuses while polling:

Status	Description for Operators	Description for Administrators
 Normal	The probe is active and running successfully.	Polling is working fine in QA NNM iSPI Performance for QA.
 Warning	The probe has returned one of the following statuses: <ul style="list-style-type: none"> • Other • Over the threshold value • Busy • Not Connected • Dropped 	The probe has returned one of the following statuses: <ul style="list-style-type: none"> • Other • Over the threshold value • Busy • Not Connected • Dropped
 Major	Indicates the metric in QA probe breaches the threshold level.	Indicates the metric in QA probe breaches the threshold level.
 Critical	The probe has returned one of the following errors: <ul style="list-style-type: none"> • Timed out error • Sequence error • Verify error • Application specific error • DNS server timeout error • TCP connect timeout error • HTTP transaction timeout error • DNS query error • HTTP error • State error • Source node or site disabled 	The probe is failing.
 Unknown	The probe has returned one of the following errors: <ul style="list-style-type: none"> • SNMP error • If there is no polling policy 	The probe is Active or Enabled
 Disabled	The probe is disabled.	The probe has returned one of the following statuses: <ul style="list-style-type: none"> • Not in service

Status	Description for Operators	Description for Administrators
		<ul style="list-style-type: none"> • Disabled
 Not Polled	When the user selected not to poll the source node	When the user selects not to poll the source node
 No Status	<ul style="list-style-type: none"> • When the node is not managed – Indicates the node is intentionally not managed. For example, certain nodes may not be managed during scheduled network maintenance cycles. HP Network Node Manager i Software does not update discovery information or monitor these nodes. • When the node is out of service – Indicates a node is unavailable because it is out of service. NNMI does not update discovery information or monitor these nodes. This attribute is useful for notifying NNMI when a device is temporarily out of service, or should never be managed. 	<ul style="list-style-type: none"> • When the node is not managed – Indicates the node is intentionally not managed. For example, certain nodes may not be managed during scheduled network maintenance cycles. NNMI does not update discovery information or monitor these nodes. • When the node is out of service – Indicates a node is unavailable because it is out of service. NNMI does not update discovery information or monitor these nodes. This attribute is useful for notifying NNMI when a device is temporarily out of service, or should never be managed.

Administrative State

The following table describes the different Administrative States for QA probes:

QA Probe State Attributes	Description
rttMonCtrlAdminStatus	<p>The status of the conceptual RTT control row. The current Administrative State contributes towards the status calculation for this QA probe.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • active¹ • notInService² • notReady³ • createAndGo⁴ • createAndWait⁵ • destroy⁶

RFC QA Probe or Juniper RPM QA Probe State Attributes	Description
pingCtlAdminStatus	<p>For RFC, the following values are supported for the Administrative State:</p> <ul style="list-style-type: none"> • Enabled⁷ • Disabled⁸

¹Indicates that the conceptual row is available for use by the managed device.

²Indicates that the conceptual row exists in the agent, but is unavailable for use by the managed device.

³Indicates that the conceptual row exists in the agent, but is missing information necessary in order to be available for use by the managed device.

⁴Supplied by a management station that wants to create a new instance of a conceptual row and to have its status automatically set to active, making it available for use by the managed device.

⁵Supplied by a management station that wants to create a new instance of a conceptual row, but not make it available for use by the managed device.

⁶Supplied by a management station that wants to delete all of the instances associated with an existing conceptual row.

⁷Attempt to activate the QA probe.

⁸Deactivate the QA probe.

Operational State

The following table describes the different Operational States for QA probes:

QA Probe State Attributes	Description
<ul style="list-style-type: none"> rttMonLatestJitterOperSense rttMonLatestRttOperSense 	<p>The rttMonLatestJitterOperSense status defines an application specific sense code for the completion status of the latest Jitter RTT operation.</p> <p>The rttMonLatestRttOperSense status defines an application sense code for the completion status of the latest RTT operation.</p> <p>The current Operational State contributes towards the status calculation for this QA probe.</p> <p>The possible values and their descriptions are given in the below table.</p>

Possible Values	Description
Other (0)	The operation is not started or completed or this object is not applicable for the probe type.
Ok(1)	A valid completion occurred and timed successfully.
disconnected(2)	The operation did not occur because the connection to the target was lost.
overThreshold(3)	A valid completion was received but the completion time exceeded a threshold value.
timeout(4)	An operation timed out; no completion time recorded.
busy(5)	The operation did not occur because a previous operation is still outstanding.
notConnected(6)	The operation did not occur because no connection (session) exists with the target.
dropped(7)	The operation did not occur due to lack of internal resource.
sequenceError(8)	A completed operation did not contain the correct sequence id; no completion time recorded.
VerifyError(9)	A completed operation was received, but the data it contained did not match the expected data; no completion time recorded.
applicationSpecific(10)	The application generating the operation had a specific error.
dnsServerTimeout(11)	DNS Server Timeout

Possible Values	Description
tcpConnectTimeout(12)	TCP Connect Timeout
httpTransactionTimeout (13)	HTTP Transaction Timeout
dnsQueryError(14)	DNS Query error (because of unknown address etc.)
httpError(15)	HTTP Response Status Code is not OK (200) then HTTP error is set.
error(16)	If there are socket failures or some other errors not relevant to the actual probe, they are recorded under this error.

RFC QA Probe or Juniper RPM QA Probe State Attributes	Description
pingResultsOperStatus	For RFC, the following Operational States are supported: <ul style="list-style-type: none"> • Enabled¹ • Disabled²

¹QA probe is active.

²QA probe has stopped.

Chapter 2: Measuring Ping Latency

The NNM iSPI Performance for QA enables you to measure the connectivity between a router and node in your network with the help of ping requests. Using a configuration file provided by the NNM iSPI Performance for QA, you can define a router-node pair to trigger ping requests from the router to the node. The NNM iSPI Performance for QA initiates ping requests originating from a source router to a destination node (defined by a router-node pair or a [ping latency pair](#)¹), collects the statistics of the ping from the router, and displays the statistics, such as round-trip time (RTT) and packet loss details, in the Ping Latency Pairs inventory view.

Note: The Ping Latency Pair feature works only with Cisco routers.

The NNM iSPI Performance for QA collects the ping statistics from the router immediately after a response for the ping request arrives. If the ping request for a router-node pair fails, the NNM iSPI Performance for QA generates an incident. The incident is closed automatically when the ping request for the router-node pair is successful.

To use this feature, you must configure ping pairs by defining source routers and destinations nodes in the `PingPair.conf` file. For more information, see ["Configuring Ping Latency Pairs" on page 151](#). You can also modify the default size and frequency of ping requests if you have administrator or root access to the NNMi management server. For more information, see ["Configuring Default Ping Attributes" on page 154](#).

Accessing the Ping Latency Pairs Inventory View

The Ping Latency Pairs inventory view enables you to view the list of configured [ping latency pair](#)²s in the network.

To launch the Ping Latency Pair Inventory view:




1. Log on to the NNMi console using your user name and password.
2. Click **Quality Assurance** in the Workspaces panel.
3. Click **Ping Latency Pairs**. The ping pair nodes that are discovered in your network appear in the content pane along with some key attributes.

Key Attributes of the Ping Latency Pair Inventory View

The Ping Latency Pairs Inventory view displays the following key attributes:

¹A router-node pair used by the NNM iSPI Performance for QA to measure and monitor the connectivity between the router and the node. The router-node pair definition must be available in a configuration file provided by the NNM iSPI Performance for QA.




²A router-node pair used by the NNM iSPI Performance for QA to measure and monitor the connectivity between the router and the node. The router-node pair definition must be available in a configuration file provided by the NNM iSPI Performance for QA.

Attribute Name	Description
Status	The status of the configured ping pair. NNM iSPI Performance for QA calculates the status based on the polling status of the ping pair nodes and the threshold states. The status can be any one of the following: <ul style="list-style-type: none"> •  Normal •  Critical •  No Status
Name	This is a combination of the FQDN of the source router and IP address of the destination node. This attribute appears in the following format: <Source_FQDN>_<Destination_IP>
Source	The name of the source node.
Source IP	The IP address of the source node.
Destination	The name of the destination node.
Destination IP	The IP address of the destination node.
Manager	Specifies whether the NNMi management server is Local or not. The name of the Regional Manager is displayed if the NNMi management server is not local.

In case of large number of Ping Latency Pairs, you can filter them based on the various QA groups. As you type, the auto-complete feature lists the matching QA Groups. You can select a QA Group name from the list.

Analysis Pane

The Analysis pane for the selected Ping Latency Pair shows the following details:

Attributes	Description
Ping Pair Details Summary	Denotes the status of the selected Ping Pair. The status can be one of the following: <ul style="list-style-type: none"> •  Normal •  Critical •  No Status
Name	The name of the ping pair that you provide during the configuration.
Threshold State	Displays if any configured thresholds are violated for the selected ping latency pair.
Latest Polled Values	Displays the following details of the source element for latest polling cycle: <ul style="list-style-type: none"> • RTT (in milliseconds)

Attributes	Description
	<ul style="list-style-type: none"> Interface utilization







Performance Tab

The **Performance** tab enables you to analyze the performance faults for the selected ping pair with the help of graphs. The graph shows the following information:

- RTT value of the selected ping pair
- Reachability of the selected ping pair
- Packet loss of the selected ping pair

You can easily monitor and analyze the performance of the ping pair from the color of the status. Whenever any problem arises, you can view the status in the **Performance** tab. The status of the ping pair enables you to easily determine the root cause of the fault.


The following table indicates the status information:

Ping Pair Status	Status color indicating in the graph
Nominal	 Normal
High, Low	 Major
Critical	 Critical
No status	 No Status
Unavailable, Unknown	 Unknown
Not Polled, Threshold not set, Not defined	 Disabled

Viewing Ping Latency Pair Details

The Ping Latency Pair Form view displays the details of a selected ping pair.

Ping Pair Details

Details	Description
Name	<p>This is a combination of the FQDN of the source router and IP address of the destination node. This attribute appears in the following format:</p> <p><Source_FQDN>_<Destination_IP></p>
Status	<p>The status of the configured ping pair. The status can be one of the following:</p> <ul style="list-style-type: none"> •  Normal

Details	Description
	<ul style="list-style-type: none">  Critical  No Status

Source Details

Details	Description
Source	The name of the source node.
Source IP	The IP address of the source node.
Source Interface	The interface name on which the source node resides.

Destination Details

Details	Description
Destination	The name of the destination node.
Destination IP	The IP address of the destination node.
Destination Interface	The interface name on which the destination node resides.



Source Proxy Details







Details	Description
Node Name	The name of the proxy source node.
IP Address	The IP address of the proxy source node.

The right pane of the Ping Latency Pair form displays the QA Groups tab. The QA Groups tab lists the groups to which the selected ping pair belongs.

Valid Ping Latency Pair Statuses

The system displays any one of the following valid Ping Latency Pairs statuses while polling:

Status	Description for Operators	Description for Administrators
 Normal	The source node is Ok or Enabled	The source node or site is Active or Enabled
 Warning	The source node has returned one of the following statuses: <ul style="list-style-type: none"> Other 	The source node or site is Active or Enabled

Status	Description for Operators	Description for Administrators
	<ul style="list-style-type: none"> • Disconnected • Over the threshold value • Busy • Not Connected • Dropped 	
 Major	Indicates the metric in QA probe breaches the threshold level.	Indicates the metric in QA probe breaches the threshold level.
 Critical	The source node has returned one of the following errors: <ul style="list-style-type: none"> • Timed out error • Sequence error • Verify error • Application specific error • DNS server timeout error • TCP connect timeout error • HTTP transaction timeout error • DNS query error • HTTP error • State error • Source node or site disabled 	The source node or site has returned one of the following statuses: <ul style="list-style-type: none"> • Not ready • Create and go • Create and wait • Destroy
 Unknown	The source node has returned one of the following errors: <ul style="list-style-type: none"> • SNMP error • If there is no polling policy 	The source node or site is Active or Enabled.
 Disabled	The source node is disabled.	The source node or site has returned one of the following statuses: <ul style="list-style-type: none"> • Not in service • Disabled
 Not Polled	Indicates that the user has selected not to poll the source node.	Indicates that the user has selected not to poll the source node.
 No Status	<ul style="list-style-type: none"> • When the node is not managed – Indicates the node is intentionally not managed. For example, certain nodes may not be managed during scheduled network maintenance cycles. HP Network Node Manager i Software does 	<ul style="list-style-type: none"> • When the node is not managed – Indicates the node is intentionally not managed. For example, certain nodes may not be managed during scheduled network maintenance cycles. NNMi does not update discovery information or monitor these nodes.

Status	Description for Operators	Description for Administrators
	<p>not update discovery information or monitor these nodes.</p> <ul style="list-style-type: none">• When the node is out of service – Indicates a node is unavailable because it is out of service. NNMi does not update discovery information or monitor these nodes. This attribute is useful for notifying NNMi when a device has been temporarily out of service, or should never be managed.	<ul style="list-style-type: none">• When the node is out of service – Indicates a node is unavailable because it is out of service. NNMi does not update discovery information or monitor these nodes. This attribute is useful for notifying NNMi when a device has been temporarily out of service, or should never be managed.

Chapter 3: Accessing QoS Details

NNM iSPI Performance for QA enables you to monitor **Quality of Service (QoS)** managed network elements available in your NNMi environment. Using NNM iSPI Performance for QA, you can monitor the health and performance of QoS managed interfaces, policies and classes. The QoS related views enable you to:

- Discover and list the QoS interfaces available in the network, and the QoS policies and actions applied on them.
- Discover and list the QoS policies configured in the network, along with the mapping between these policies, classes and QoS interfaces.
- Monitor the threshold state and raise incidents for the breached thresholds.

NNM iSPI Performance for QA supports Cisco CBQoS interfaces and nodes. NNM iSPI Performance for QA uses the CISCO-CLASS-BASED-QOS-MIB to collect the CBQoS performance data.



Viewing QoS Interface Details

The QoS Interfaces inventory view enables you to view the list of discovered interfaces for which the QoS Policies are configured. The traffic can be ingress or egress for an interface.



To launch the QoS Interfaces Inventory view:

1. Log on to NNMi console using your user name and password.
2. Click **Quality Assurance** in the Workspaces panel. The Quality Assurance tab expands.
3. Click **QoS Interfaces**. The QoS-enabled interfaces that are discovered in your network appear along with some key attributes in the content pane. By default, this information is refreshed every 300 seconds, or 5 minutes.

To view the Interface Inventory for a selected interface:

1. Select an interface in the QoS Interfaces Inventory view and click  **Open**. The Interface form appears.
2. In the QoS Interface form, click  **Lookup** that is next to the Interface Name field to open the Interface form for the selected interface.

You can open the QoS Interfaces Inventory view using the Nodes Inventory view. To open the QoS Interface Inventory view:

1. Select **Inventory** in the Workspaces panel.
2. Select **Nodes**.
3. Select a node and click  **Open**.
4. In the Node form, select QoS Interfaces tab.
5. Select a QoS interface and click  **Open** to open the QoS Interfaces Inventory view.

Key Attributes of the QoS Interfaces Inventory View

The QoS Interfaces Inventory view displays the following key attributes:

Attribute Name	Description
Interface Name	The name of the interface.
Hosted on Node	The name of the node on which the interface resides.
In Policy	The name of the In policy ¹ associated with the interface. This attribute displays only the parent policy ² name.
Out Policy	The name of the Out policy ³ associated with the interface. This attribute displays only the parent policy ⁴ name.
Applied On	The interface on which the policy is applied. Possible values are: <ul style="list-style-type: none"> Control Plane Interface Sub Interface (Only for Juniper devices)
Tenant	Specifies the NNMi tenant selected for the interface.
Management Server	Specifies whether the NNMi management server is local or not. The name of the Regional Manager is displayed if the NNMi management server is not local.
Management Mode	Specifies whether the source node is managed or not. Possible states are: <ul style="list-style-type: none"> Managed: Indicates that the node is managed. Not Managed: Indicates that the node is not managed on purpose. Out of Service: Indicates that a node is unavailable because it is out of service.

If there are large number of QoS interfaces, you can filter the interfaces based on the various QA groups. As you type, the auto-complete feature lists the matching QA Groups. You can select a QA Group name from the list.

You can filter the interfaces listed in this view based on all columns of this view. However, make sure that you apply filter on either the In Policy or the Out Policy column. If you apply filter on both the

¹In Policy defines the policy which is applied to the incoming traffic.

²The policy that contains references to other policy configurations. NNM iSPI Performance for QA displays only one hierarchical level for policies. For example, Policy1 contains references for Policy2 and NNM iSPI Performance for QA considers Policy2 as the child policy of Policy1. If Policy2 contains references to Policy3, the inventory views do not display Policy3 as a child of Policy1.

³Out Policy defines the policy which is applied to the outgoing traffic.

⁴The policy that contains references to other policy configurations. NNM iSPI Performance for QA displays only one hierarchical level for policies. For example, Policy1 contains references for Policy2 and NNM iSPI Performance for QA considers Policy2 as the child policy of Policy1. If Policy2 contains references to Policy3, the inventory views do not display Policy3 as a child of Policy1.

columns, then the NNM iSPI Performance for QA discards both the filters and applies a filter that you may have configured for the other columns.


If you apply the filter 'Not Equal To This Value' on either the In Policy or the Out Policy columns, then the NNM iSPI Performance for QA filters out the following interfaces:

- Interfaces whose in policy or out policy names do not match the filter value.
- Interfaces whose in policy or out policy values are NULL.

In Policy

The **In Policy** tab displays information about the policies applied on the incoming traffic of the selected interface. It displays the policy information for the [parent policy](#)¹ as well as the [child policy](#)².

Attributes: In Policy Details Tab

Attribute	Description
Action	The name of a QoS action. The QoS action can be one of the following: <ul style="list-style-type: none">• Queuing• Policing• Shaping• Packet Marking• RED
Traffic Class Name	Name of a Traffic Class mapped to the policy. Click  Lookup next to the In Policy and the Out Policy fields to view information on the policies associated with the traffic class. For more information about QoS class map for a selected traffic class, see " QoS Class Map Form " on page 75.

Out Policy


The **Out Policy** tab displays information about the policies applied on the outgoing traffic of the selected interface.

¹The policy that contains references to other policy configurations. NNM iSPI Performance for QA displays only one hierarchical level for policies. For example, Policy1 contains references for Policy2 and NNM iSPI Performance for QA considers Policy2 as the child policy of Policy1. If Policy2 contains references to Policy3, the inventory views do not display Policy3 as a child of Policy1.

²The policy that the parent policy refers to.

The Out Policy tab displays the policy information for the [parent policy](#)¹ as well as the [child policy](#)².

Attributes: Out Policy Details Tab

Attribute	Description
Action	The name of a QoS action. The QoS action can be one of the following: <ul style="list-style-type: none">• Queuing• Policing• Shaping• Packet Marking• RED
Traffic Class Name	Name of a Traffic Class mapped to the policy. Click  Lookup that is next to In Policy and the Out Policy fields to view information on the policies associated with the traffic class. To view the QoS class map details for the selected traffic class, see " QoS Class Map Form " on page 75.

Threshold State

The **Threshold State** tab displays information about the discovered threshold states for the selected interface.

It displays the threshold states for the [parent policy](#)³ as well as the [child policy](#)⁴.

The threshold defined on a policy is applied to all the classes configured for the policy. Even if you do not configure any action for a class of a policy, but configure a threshold for the policy, NNM iSPI Performance for QA applies the threshold on every class and displays them in the Threshold State tab. For example, if you have not defined an action for the Class-Default for a policy, but configured a threshold on the policy, NNM iSPI Performance for QA displays Class-Default in the Threshold State tab.





¹The policy that contains references to other policy configurations. NNM iSPI Performance for QA displays only one hierarchical level for policies. For example, Policy1 contains references for Policy2 and NNM iSPI Performance for QA considers Policy2 as the child policy of Policy1. If Policy2 contains references to Policy3, the inventory views do not display Policy3 as a child of Policy1.

²The policy that the parent policy refers to.

³The policy that contains references to other policy configurations. NNM iSPI Performance for QA displays only one hierarchical level for policies. For example, Policy1 contains references for Policy2 and NNM iSPI Performance for QA considers Policy2 as the child policy of Policy1. If Policy2 contains references to Policy3, the inventory views do not display Policy3 as a child of Policy1.

⁴The policy that the parent policy refers to.

Attributes: Threshold State Tab


Attribute	Description
State	Threshold state for the QoS elements. Can be one of the following values: <ul style="list-style-type: none"> • High:¹ • Nominal:² • Not Defined:³
Metric	Name of the metric that has crossed the threshold state for the configured QoS interface.
Direction	Indicates whether the threshold was applied on the incoming or outgoing traffic for the selected interface.
Traffic Class Name	Displays the name of a Traffic Class mapped to the policy. Click  Lookup next to the In Policy and the Out Policy fields to view information on the policies associated with the traffic class. To view the QoS Class Details for the selected traffic class, follow these steps: <ol style="list-style-type: none"> 1. Click  Lookup next to the In Policy or Out Policy fields. 2. Select  Open to open the QoS Policy form. 3. Select Traffic Classes tab, select a traffic class and click  Open to open the QoS Class Map form. This form displays the action definitions associated with a class. For example, if the queuing action is configured for Class A, the QoS Class Map form displays a tab for queuing action. The tab displays the properties and the value for each property. The values for these properties are measured in bits per second (bps). This form does not display the details for nested classes.
Type	Type of the threshold set for the metric. Can be of the following types: <ul style="list-style-type: none"> • Count: ⁴ • Time: ⁵

¹ Specifies that the metric value for the QoS policy crossed the configured threshold value.
² Specifies that the metric value for the QoS policy is within the configured threshold value.
³ Specifies that the threshold was configured, but NNM iSPI Performance for QA did not poll the device.
⁴ NNM iSPI Performance for QA raises an incident only if the threshold for the configured QoS policy is crossed for a pre-specified number of times consecutively.
⁵ NNM iSPI Performance for QA raises an incident only if the metric value is beyond the threshold value for a pre-specified time period.

Attributes: Threshold State Tab, continued

Attribute	Description
High Value	Threshold value that the administrator has configured for the policy. NNM iSPI Performance for QA raises an incident when the metric value crosses the configured threshold value and sets the threshold state to High.
High Value Rearm	Rearm value that the administrator has configured for the policy. NNM iSPI Performance for QA raises an incident when the metric value crosses the configured threshold value. When the metric value reaches the rearm value, NNM iSPI Performance for QA clears the incident and sets the threshold state to Nominal.










Each time the NNM iSPI Performance for QA starts running on the Global Manager, the Global Manager pulls the changed threshold states from all Regional Managers since the last run of NNM iSPI Performance for QA. The Global Manager then raises incidents for the overall health of the configured QoS policies in the network, based on these threshold states. However, the Global Manager does not display the threshold values configured in the Regional Managers.

To view the details about a threshold, select a threshold and click  **Open** and display the Threshold State Details form.







QoS Interfaces Form: Incidents Tab

The Incidents tab displays information on the incidents raised on the selected interface.

Attributes: Incidents Tab

Attribute	Description
Severity	Seriousness that NNMi calculates for the incident. Possible values are: <ul style="list-style-type: none"> •  Normal •  Warning •  Minor •  Major •  Critical •  Unknown •  Disabled •  Not Polled •  No Status
Lifecycle State	Identifies where the incident is in the incident lifecycle.
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

Attributes: Incidents Tab, continued

Attribute	Description
	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.
Correlation Nature	This incident's contribution to a root-cause calculation, if any.
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 for more information about the node.
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 the Node Form for more information about the object.
Message	The incident message defined by NNMi.

The global manager raises incidents for the overall health of the configured QoS interfaces in the network, based on the threshold states collected from all regional managers.

For detailed information on NNMi incidents, see *Incident Form* topic in HP Network Node Manager i Software *Help for Operators*.

QoS In or Out Policy

The QoS In or Out Policy form displays the following details:

- Traffic Class name: Name of the Traffic Class mapped to the policy.
- Action: Type of action applied to the policy and associated with the Traffic Class.

Analysis Pane







The Analysis Pane shows the details of the selected QoS Interface, such as, Interface Name, Interface Description, Interface Speed, In Policy, and Out Policy.

The **Performance** panel enables you to analyze the performance faults for the selected QoS Interface, in the form of graphs. The graph shows the following information:

- Interface utilization of the selected QoS Interface.
- Availability of the selected QoS Interface. It denotes whether the interface is active or not.

You can easily monitor and analyze the performance of the QoS Interface, from the color of the status. Whenever any problem arises, you can view the status in the **Performance** panel. The status of the probe enables you to easily determine the root cause of the fault.

The following table indicates the status information:

QoS Interface Status	Status color indicating in the graph
Nominal, NOMINAL	 Normal
High, Low	 Major
Critical	 Critical
No status	 No Status
UNAVAILABLE, UNKNOWN	 Unknown
NOT POLLED, Not Polled, Threshold not set, Not defined	 Disabled

The Traffic Classes tab on the QoS Interfaces Inventory displays the information on the set of Traffic Classes, Policy name and the QoS actions implemented.

For the interfaces on the Juniper devices, the tab also displays the queue number to which the each traffic (forwarding) class belongs.

The possible QoS actions are Policing, Shaping, Queueing, Packet Marking, and RED.

Viewing QoS Policy Details

The QoS Policies Inventory view enables you to view the QoS policies that are configured on the interfaces and the type of [QoS Actions](#) applied on it.

To launch the QoS Policies Inventory view:

1. Log on to NNMi console using your user name and password.
2. Click **Quality Assurance** in the Workspaces panel. The Quality Assurance tab expands.
3. Click **QoS Policies**. The QoS enabled policies that are discovered in your network appear in the content pane along with some key attributes. By default, this information is refreshed every 300 seconds, or 5 minutes.

Key Attributes of the QoS Policies Inventory View

The QoS Policies Inventory view displays the following key attributes:

Attribute Name	Description
Policy Name	The name of the policy applied. By default, this attribute displays only the parent policy ¹ name. This attribute displays the child policy ² , only if the child policy is directly applied on an interface. This attribute does not display a child policy, if it is referred to by multiple parent policies.
Applied on Interfaces	The total number of interfaces to which the policy is mapped.
Hosted on Node	The name of the node on which the interface mapped to the selected policy resides.
Policing	Indicates that the "Policing" action is configured for one or more traffic classes associated with the selected policy.
Shaping	Indicates that the "Shaping" action is configured for one or more traffic classes associated with the selected policy.
Queuing	Indicates that the "Queuing" action is configured for one or more traffic classes associated with the selected policy.
Packet Marking	Indicates that the "Packet Marking" action is configured for one or more traffic classes associated with the selected policy.



¹The policy that contains references to other policy configurations. NNM iSPI Performance for QA displays only one hierarchical level for policies. For example, Policy1 contains references for Policy2 and NNM iSPI Performance for QA considers Policy2 as the child policy of Policy1. If Policy2 contains references to Policy3, the inventory views do not display Policy3 as a child of Policy1.

²The policy that the parent policy refers to.

Attribute Name	Description
RED	Indicates that the "RED" action is configured for one or more traffic classes associated with the selected policy.
Tenant	Specifies the NNMi tenant selected for the selected policy.
Management Server	Specifies whether the NNMi management server is local or specifies the name of the regional manager.
Management Mode	Specifies whether the source node is managed or not. Possible states are as follows: <ul style="list-style-type: none"> Managed: Indicates that the node is managed. Not Managed: Indicates that the node is not managed on purpose. Out of Service: Indicates that a node is unavailable because it is out of service.

You can filter the policies listed in this view based on all the columns.

To view a selected QoS Policy:

1. In the QoS Policies Inventory View, select a QoS policy and click  **Open**. The QoS Policy Form appears.
2. In the QoS Policy form, you can view the following information on the selected policy:
 - Interface: Displays the interface on which the policy is configured. Select the interface and click  **Open** to open the QoS Interfaces Inventory View for the selected interface.
 - Traffic Classes: Displays the traffic classes configured for the selected policy. For more information, see "[Traffic Classes](#)" on the next page.

Interfaces

The **Interface** tab displays information about the discovered interfaces for which the QoS policies are configured.

Attributes: Interface Tab

Attribute	Description
Interface Name	The name of interface.
Hosted On Node	The name of the node on which the interface resides.
In Policy	The name of the In policy ¹ associated with the interface.
Out Policy	The name of the Out policy ² associated with the interface.

¹In Policy defines the policy which is applied to the incoming traffic.

²Out Policy defines the policy which is applied to the outgoing traffic.

Attributes: Interface Tab, continued





Attribute	Description
Applied On	The interface on which the policy is applied. Possible values are: <ul style="list-style-type: none"> Control Plane Interface Sub Interface
Management Server	Specifies whether the NNMi management server is local or specifies the name of the regional manager.

Traffic Classes

The **Traffic Classes** tab displays the information about the set of Traffic Class names and the QoS actions implemented on it.

For a [parent policy](#)¹, the Traffic Classes tab displays the class configurations for the parent policy as well as the [child policy](#)².

Attributes: Traffic Classes Tab

Attribute	Description
Traffic Class Name	<p>Displays the name of a Traffic Class mapped to the policy.</p> <p>Click  Lookup next to the In Policy and the Out Policy fields to view information on the policies associated with the traffic class.</p> <p>To view the QoS Class Details for the selected traffic class, follow these steps:</p> <ol style="list-style-type: none"> 1. Click  Lookup next to the In Policy or Out Policy fields. 2. Select  Open to open the QoS Policy form. 3. Select Traffic Classes tab, select a traffic class and click  Open to open the QoS Class Map form. This form displays the action definitions associated with a class. <p>For example, if the queuing action is configured for Class A, the QoS Class Map form displays a tab for queuing action. The tab displays the properties and the value for each property. The values for these properties are measured in bits per second (bps).</p>

¹The policy that contains references to other policy configurations. NNM iSPI Performance for QA displays only one hierarchical level for policies. For example, Policy1 contains references for Policy2 and NNM iSPI Performance for QA considers Policy2 as the child policy of Policy1. If Policy2 contains references to Policy3, the inventory views do not display Policy3 as a child of Policy1.

²The policy that the parent policy refers to.

Attributes: Traffic Classes Tab, continued

Attribute	Description
	This form does not display the details for nested classes.
Policy Name	Displays the name of the policy for which you have defined the class. You can use this attribute to identify the policy name for nested policies. For example, you have defined Policy1 as the parent policy. Policy2 and Policy21 are children of Policy1. The Traffic Classes tab displays the classes defined for Policy1, Policy2, and Policy21; the Policy Name attribute displays the names of the policies for each class.
Policing	Indicates that the "Policing" action is configured for one or more traffic classes associated with the selected policy.
Shaping	Indicates that the "Shaping" action is configured for one or more traffic classes associated with the selected policy.
Queuing	Indicates that the "Queuing" action is configured for one or more traffic classes associated with the selected policy.
Packet Marking	Indicates that the "Packet Marking" action is configured for one or more traffic classes associated with the selected policy.
RED	Indicates that the "RED" action is configured for one or more traffic classes associated with the selected policy.

You can sort the data displayed in this tab based on all the above attributes.

QoS Policy Hierarchy

The QoS Policy Hierarchy tab displays the hierarchical details of the selected policy. The QoS Policy Hierarchy tab appears only for a policy that contains references to other policies. In other words, the QoS Policy form displays this tab for only a parent policy.

Attributes: QoS Policy Hierarchy Tab

Attribute	Description
Policy Name	The name of the parent or child policy.
Direct Parent Policy	The name of the parent policy.
Hierarchy Level	The hierarchy level of the policy. For a parent policy, this attribute displays 0 For a child policy, this attribute displays 1

To view the traffic class associated with the selected QoS child policy, follow the below steps:

1. In the QoS Policy Hierarchy Tab, select a QoS child policy.

2. Click  **Open**.

The QoS Policy Hierarchy form opens displaying the traffic classes configured for the selected policy. For more information, see "[Traffic Classes](#) " on page 66.

Viewing QoS Actions Details

The QoS Actions inventory view enables you to view the overview of QoS Actions that are applied to interfaces based on a particular traffic flow and a policy (Incoming and Outgoing traffic).







This view displays actions configured for the [parent policy](#)¹ as well as the [child policy](#)². However, the view lists all actions under the parent policy name and does not display the child policy name.

To launch the QoS Actions Inventory view:

1. Log on to NNMi console using your user name and password.
2. Click **Quality Assurance** in the Workspaces panel. The Quality Assurance tab expands.
3. Click **QoS Actions**. The QoS enabled actions that are discovered in your network appear in the content pane along with some key attributes. By default, this information is refreshed every 300 seconds, or 5 minutes.










Key Attributes of the QoS Actions Inventory View

The QoS Actions Inventory view displays the following key attributes:

Attribute Name	Description						
State	<p>The threshold state for the action.</p> <p>Can be one of the following values:</p> <p>Threshold States</p> <table border="1"> <thead> <tr> <th>State</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td> High</td> <td> <p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and this high value persists for the specified High Duration within the High Duration Window.</p> </td> </tr> <tr> <td> Nominal</td> <td>Indicates that the measured value of the metric is within the normal healthy range.</td> </tr> </tbody> </table>	State	Description	 High	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and this high value persists for the specified High Duration within the High Duration Window.</p>	 Nominal	Indicates that the measured value of the metric is within the normal healthy range.
State	Description						
 High	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and this high value persists for the specified High Duration within the High Duration Window.</p>						
 Nominal	Indicates that the measured value of the metric is within the normal healthy range.						

¹The policy that contains references to other policy configurations. NNM iSPI Performance for QA displays only one hierarchical level for policies. For example, Policy1 contains references for Policy2 and NNM iSPI Performance for QA considers Policy2 as the child policy of Policy1. If Policy2 contains references to Policy3, the inventory views do not display Policy3 as a child of Policy1.

²The policy that the parent policy refers to.


Attribute Name	Description								
	<p>Threshold States, continued</p> <table border="1" data-bbox="545 331 1382 951"> <thead> <tr> <th data-bbox="545 331 787 388">State</th> <th data-bbox="792 331 1382 388">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="545 394 787 478">  Unavailable </td> <td data-bbox="792 394 1382 478">Unable to compute the metric or the computed value is outside the valid range.</td> </tr> <tr> <td data-bbox="545 485 787 569">  Threshold Not Set </td> <td data-bbox="792 485 1382 569">Indicates that the threshold is not set for the metric.</td> </tr> <tr> <td data-bbox="545 575 787 951">  None </td> <td data-bbox="792 575 1382 951"> <p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero and this zero value persists for the specified duration within the High or Low Duration Window (depending on the metric).</p> </td> </tr> </tbody> </table>	State	Description	 Unavailable	Unable to compute the metric or the computed value is outside the valid range.	 Threshold Not Set	Indicates that the threshold is not set for the metric.	 None	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero and this zero value persists for the specified duration within the High or Low Duration Window (depending on the metric).</p>
State	Description								
 Unavailable	Unable to compute the metric or the computed value is outside the valid range.								
 Threshold Not Set	Indicates that the threshold is not set for the metric.								
 None	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero and this zero value persists for the specified duration within the High or Low Duration Window (depending on the metric).</p>								
Action	<p>The type of Action applied. Possible values are:</p> <ul style="list-style-type: none"> • Policing • Shaping • Queuing • Packet Marking • RED 								
Traffic Class Name	Name of the Traffic Class associated with the selected action.								
Policy Name	The name of the policy applied.								
Direction	Indicates whether the policy was applied on the incoming or outgoing traffic for an interface.								
Queue Number	<p>Indicates the queue number to which the traffic (forwarding) class (on which the action is configured) is associated.</p> <p>This field is applicable only for Juniper devices.</p>								
Interface Name	The name of the interface mapped to the QoS action.								
Hosted On Node	The name of the node on which the interface resides.								
Tenant	Specifies the NNMi tenant selected for the node (specified in Hosted On Node attribute).								
Management Server	Specifies whether the NNMi management server is local or specifies the name of the regional manager.								

Attribute Name	Description
Management Mode	Specifies whether the source node is managed or not. Possible states are as follows: <ul style="list-style-type: none"> • Managed: Indicates that the node is managed. • Not Managed: Indicates that the node is not managed on purpose. • Out of Service: Indicates that a node is unavailable because it is out of service.



You can filter the QoS actions listed in this view based on all columns except the Traffic Class Name column.

If there are large number of QoS actions, you can filter the actions based on the various QA groups. As you type, the auto-complete feature lists the matching QA Groups. You can select a QA Group name from the list.

To view a selected QoS Action:

1. In the QoS Actions Inventory View, select a QoS action.
2. Click  **Open**. The QoS Action Form appears.

In the QoS Action form, you can view the following information on the selected action:

- Interface: This tab displays the interface on which the action is configured. Select the interface and click  **Open** to open the QoS Interfaces Inventory View for the selected interface.
- QoS Policies: This tab displays the policy that is associated with the action. Select a policy and click  **Open** to open the QoS Policies Inventory View for the selected policy

The Analysis panel of the QoS Action view displays the Threshold States tab. This tab displays the details about the states of the thresholds configured on the interface. For more information about the Threshold States tab, see "[Threshold States](#) " on page 73.

Interfaces

The **Interface** tab in the QoS Actions form displays information about the interfaces for which the selected QoS action is configured.

Attributes: Interface Tab

Attribute	Description
Interface Name	The name of interface.
Hosted On Node	The name of the node on which the interface resides.
In Policy	The name of the In policy ¹ associated with the interface.

¹In Policy defines the policy which is applied to the incoming traffic.



Attributes: Interface Tab, continued

Attribute	Description
Out Policy	The name of the Out policy ¹ associated with the interface.
Applied On	The interface on which the policy is applied. Possible values are: <ul style="list-style-type: none"> Control Plane Interface
Tenant	Specifies the NNMi tenant selected for the interface.
Management Server	Specifies whether the NNMi management server is local or specifies the name of the regional manager.
Management Mode	Specifies whether the source node is managed or not. Possible states are as follows: <ul style="list-style-type: none"> Managed: Indicates that the node is managed. Not Managed: Indicates that the node is not managed on purpose. Out of Service: Indicates that a node is unavailable because it is out of service.

QoS Policies

The **QoS Policies** tab in the QoS Actions form displays information about the interfaces and QoS policies mapped to the selected QoS action.

Attributes: QoS Policies Tab

Attribute	Description
Policy Name	The name of the policy mapped to the selected QoS action. To view the interfaces and traffic classes associated with the selected policy, click  Open after selecting a policy. To view the QoS class map details for the selected traffic class, select a traffic class in the Traffic Class tab of the QoS Policy form, and click  Open . The QoS Class Map form does not display the details for nested classes.
Applied on Interfaces	The total number of interfaces to which the selected QoS policy is mapped.
Hosted on Node	The name of the node on which the interface mapped to the selected policy resides.
Policing	Indicates that the "Policing" action is configured for one or more traffic classes

¹Out Policy defines the policy which is applied to the outgoing traffic.

Attributes: QoS Policies Tab, continued

Attribute	Description
	associated with the selected policy.
Shaping	Indicates that the "Shaping" action is configured for one or more traffic classes associated with the selected policy.
Queuing	Indicates that the "Queuing" action is configured for one or more traffic classes associated with the selected policy.
Packet Marking	Indicates that the "Packet Marking" action is configured for one or more traffic classes associated with the selected policy.
RED	Indicates that the "RED" action is configured for one or more traffic classes associated with the selected policy.
Tenant	Specifies the NNMi tenant selected for the selected policy.
Management Server	Specifies whether the NNMi management server is local or specifies the name of the regional manager.
Management Mode	Specifies whether the source node is managed or not. Possible states are as follows: <ul style="list-style-type: none"> • Managed: Indicates that the node is managed. • Not Managed: Indicates that the node is not managed on purpose. • Out of Service: Indicates that a node is unavailable because it is out of service.

Threshold States

The **Threshold State** tab in the Analysis pane displays information about the discovered threshold states for the selected QoS interfaces and policies.

An administrator can set the thresholds to monitor the health and performances of the configured QoS policies. For more information about setting up thresholds for configured QoS policies, see ["Configuring QoS Thresholds" on page 270](#).

Attributes: Threshold States Tab

Attribute	Description
Metric	Name of the metric that has crossed the threshold state for the configured QoS interface.
Threshold State	Threshold state for the QoS elements. Can be of the following values:

Attributes: Threshold States Tab, continued

Attribute	Description
	<ul style="list-style-type: none">• High¹• Nominal²
Type	Type of the threshold set for the metric. Can be of the following types: <ul style="list-style-type: none">• Count³• Time⁴
Configured	Threshold value that the administrator has configured for the policy. NNM iSPI Performance for QA raises an incident when the metric value crosses the configured threshold value and sets the threshold state to High.
Rearm	Rearm value that the administrator has configured for the policy. NNM iSPI Performance for QA raises an incident when the metric value crosses the configured threshold value. When the metric value reaches the rearm value, NNM iSPI Performance for QA clears the incident and sets the threshold state to Nominal.

Each time the NNM iSPI Performance for QA starts running on the Global Manager, the Global Manager pulls the changed threshold states from all Regional Managers since the last run of NNM iSPI Performance for QA. The Global Manager then raises incidents for the overall health of the configured QoS policies in the network, based on these threshold states.

Quality of Service (QoS) Actions

The QoS actions are listed below:

Traffic Queuing

The Queuing action is required only when the interface is busy. Typical queuing is based on the First in First Out (FIFO) principle wherein the packet that has been waiting for the longest period is transmitted first. This results in a tail drop once the queue is full. To override this, you can specify the queuing algorithm, which is the deciding factor to determine which packet must be transmitted first in the queue. There are several queuing strategies, such as WFQ, Random Early Detector (RED), priority, and custom queuing. You can also specify the bandwidth allotted, and the maximum allowed queue size for the traffic class.

¹Specifies that the metric value for the QoS policy crossed the configured threshold value.

²Specifies that the metric value for the QoS policy is within the configured threshold value.

³NNM iSPI Performance for QA raises an incident only if the threshold for the configured QoS policy has crossed for a pre-specified number of times consecutively.

⁴NNM iSPI Performance for QA raises an incident only if the metric value is beyond the threshold value for a pre-specified time period.

Traffic Policing

Traffic Policing is the process of dropping or discarding packets in a traffic stream, in accordance with the corresponding meter, which enforces a traffic flow.

Traffic Shaping

Traffic Shaping is the process of delaying the packet within a traffic stream, in order to conform to some of the defined traffic profiles/flows. You can specify the committed traffic-shaping rate, burst size, excess burst size, adaptive traffic shaping rate (if enabled) and the limit type (peak rate / average rate).

Traffic Marking

Traffic Marking involves setting or changing one or more attributes of the traffic that belongs to a specific traffic class. Traffic Marking can be defined as the process of setting a Differentiated Services (DS) code point on a packet, in accordance with the defined rules.

RED




Random Early Detect (RED) is also known as random early drop or random early discard. RED mechanism can be applied on network components, to ensure better results during network congestion. During a network congestion, a network component (example: Router) buffers maximum packets, and drops other packets, which cannot be buffered. RED mechanism estimates the average queue size and decides which packets are to be dropped. By using the RED algorithm, it is ensured that all important packets reach the destination.

QoS Class Map Form

Displays the name of a Traffic Class mapped to the policy.

Click  **Lookup** next to the In Policy and the Out Policy fields to view information on the policies associated with the traffic class.

To view the QoS Class Details for the selected traffic class, follow these steps:

1. Click  **Lookup** next to the In Policy or Out Policy fields.
2. Select  **Open** to open the QoS Policy form.
3. Select **Traffic Classes** tab, select a traffic class and click  **Open** to open the QoS Class Map form. This form displays the action definitions associated with a class.

For example, if the queuing action is configured for Class A, the QoS Class Map form displays a tab for queuing action. The tab displays the properties and the value for each property. The values for these properties are measured in bits per second (bps).

This form does not display the details for nested classes.

Identifying QoS Interfaces with Threshold Exceptions

The QoS Interfaces Threshold Exceptions inventory view enables you to view the list of QoS interfaces for which any of the following actions crossed the threshold and NNM iSPI Performance for QA raised an

exception:

- Packet Marking
- Policing
- Queuing
- Shaping
- RED

For information about each of the above listed actions, see ["Quality of Service \(QoS\) Actions" on page 74](#).

To launch the QoS Interfaces Threshold Exceptions inventory view:

1. Log on to NNMi console using your user name and password.
2. Click **Quality Assurance** in the Workspaces panel. The Quality Assurance tab expands.
3. Click **QoS Interfaces Threshold Exceptions**. The QoS interfaces that crossed the threshold for an action appear in the content pane along with some key attributes. By default, this information is refreshed every 300 seconds, or 5 minutes.

The QoS Threshold Exceptions Interfaces Inventory view displays the following key attributes:






Attribute Name	Description
Interface Name	The name of interface.
Hosted on Node	The name of the node on which the interface resides.
Policy Name	The name of the policy applied on the selected interface. By default, this attribute displays only the parent policy ¹ name.
Direction	Indicates whether the policy is applied on the incoming traffic or outgoing traffic for the selected interface.
Traffic Class Name	Name of an associated Traffic Class, based on a specific criterion.
Class State	The threshold state for the thresholds configured on the traffic class.
Packet Marking	Indicates the threshold state for the "Packet Marking" action configured for one or more traffic classes associated with the selected policy.
Policing	Indicates the threshold state for the "Policing" action configured for one or more traffic classes associated with the selected policy.
Queuing	Indicates the threshold state for the "Queuing" action configured for one or more traffic classes associated with the selected policy.

¹The policy that contains references to other policy configurations. NNM iSPI Performance for QA displays only one hierarchical level for policies. For example, Policy1 contains references for Policy2 and NNM iSPI Performance for QA considers Policy2 as the child policy of Policy1. If Policy2 contains references to Policy3, the inventory views do not display Policy3 as a child of Policy1.

Attribute Name	Description
Shaping	Indicates the threshold state for the "Shaping" action configured for one or more traffic classes associated with the selected policy.
RED	Indicates the threshold state for the "RED" action configured for one or more traffic classes associated with the selected policy.
Tenant	Indicates the NNMi tenant selected for the node (specified in Hosted On Node attribute).
Management Server	Specifies whether the NNMi management server is Local or not. The name of the Regional Manager is displayed if the NNMi management server is not local.


The actions and class states show the following threshold states:

Threshold States

State	Description
 High	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and this high value persists for the specified High Duration within the High Duration Window.</p>
 Nominal	Indicates that the measured value of the metric is within the normal healthy range.
 Unavailable	Unable to compute the metric or the computed value is outside the valid range.
 Threshold Not Set	Indicates that the threshold is not set for the metric.
 None	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero and this zero value persists for the specified duration within the High or Low Duration Window (depending on the metric).</p>

If there are large number of QoS interfaces that crossed the threshold, you can filter those interfaces based on the various QA groups. As you type, the auto-complete feature lists the matching QA Groups. You can select a QA Group name from the list.

The view shows threshold states for the traffic class and five different actions: Packet Marking, Policing, Queuing, Shaping, and RED. An interface appears in this view if at least one of the above thresholds is violated for the interface.

To open the QoS Interface inventory view for an interface, select the interface and click  **Open**. For information about QoS Interface inventory view, see ["Viewing QoS Interface Details" on page 56](#).

You can filter the interfaces listed in this view based on all columns of this view.

Accessing the QoS Actions Threshold Exceptions Inventory View







The QoS Actions Threshold Exceptions inventory view enables you to view the list of QoS actions that crossed the threshold and NNM iSPI Performance for QA raised an exception.










For more information about actions, see ["Quality of Service \(QoS\) Actions" on page 74](#).

To launch the QoS Threshold Exceptions Actions Inventory view:

1. Log on to NNMi console using your user name and password.
2. Click **Quality Assurance** in the Workspaces panel.
3. Click **QoS Actions Threshold Exceptions**. The QoS actions that crossed the threshold appear in the content pane along with some key attributes. By default, this information is refreshed every 300 seconds, or 5 minutes.

The QoS Threshold Exceptions Actions Inventory view displays the following key attributes:

Attribute Name	Description						
State	<p>The threshold state for the action.</p> <p>Can be any of the following values:</p> <p>Threshold States</p> <table border="1" data-bbox="444 1346 1377 1843"> <thead> <tr> <th data-bbox="444 1346 686 1402">State</th> <th data-bbox="686 1346 1377 1402">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="444 1402 686 1780">  High </td> <td data-bbox="686 1402 1377 1780"> <p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and this high value persists for the specified High Duration within the High Duration Window.</p> </td> </tr> <tr> <td data-bbox="444 1780 686 1843">  Nominal </td> <td data-bbox="686 1780 1377 1843"> <p>Indicates that the measured value of the metric is within</p> </td> </tr> </tbody> </table>	State	Description	 High	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and this high value persists for the specified High Duration within the High Duration Window.</p>	 Nominal	<p>Indicates that the measured value of the metric is within</p>
State	Description						
 High	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and this high value persists for the specified High Duration within the High Duration Window.</p>						
 Nominal	<p>Indicates that the measured value of the metric is within</p>						






Attribute Name	Description										
	<p>Threshold States, continued</p> <table border="1" data-bbox="444 367 1377 1045"> <thead> <tr> <th data-bbox="444 367 686 422">State</th> <th data-bbox="686 367 1377 422">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="444 422 686 478"></td> <td data-bbox="686 422 1377 478">the normal healthy range.</td> </tr> <tr> <td data-bbox="444 478 686 573">  Unavailable </td> <td data-bbox="686 478 1377 573">Unable to compute the metric or the computed value is outside the valid range.</td> </tr> <tr> <td data-bbox="444 573 686 667">  Threshold Not Set </td> <td data-bbox="686 573 1377 667">Indicates that the threshold is not set for the metric.</td> </tr> <tr> <td data-bbox="444 667 686 1045">  None </td> <td data-bbox="686 667 1377 1045"> <p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero and this zero value persists for the specified duration within the High or Low Duration Window (depending on the metric).</p> </td> </tr> </tbody> </table>	State	Description		the normal healthy range.	 Unavailable	Unable to compute the metric or the computed value is outside the valid range.	 Threshold Not Set	Indicates that the threshold is not set for the metric.	 None	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero and this zero value persists for the specified duration within the High or Low Duration Window (depending on the metric).</p>
State	Description										
	the normal healthy range.										
 Unavailable	Unable to compute the metric or the computed value is outside the valid range.										
 Threshold Not Set	Indicates that the threshold is not set for the metric.										
 None	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero and this zero value persists for the specified duration within the High or Low Duration Window (depending on the metric).</p>										
Action	The name of the action that crossed the threshold.										
Traffic Class Name	Name of an Traffic Class associated with the selected action.										
Policy Name	<p>The name of the policy associated with the selected action.</p> <p>By default, this attribute displays only the parent policy¹ name.</p>										
Direction	Indicates whether the policy is applied on the incoming traffic or outgoing traffic for the selected interface.										
Interface Name	The name of the interface associated with the selected action										
Hosted on Node	The name of the node on which the interface resides										
Tenant	Specifies the NNMi tenant selected for the node (specified in Hosted On Node attribute)										
Management Server	Specifies whether the NNMi management server is Local or not. The name of the Regional Manager is displayed if the NNMi management server is not local.										


¹The policy that contains references to other policy configurations. NNM iSPI Performance for QA displays only one hierarchical level for policies. For example, Policy1 contains references for Policy2 and NNM iSPI Performance for QA considers Policy2 as the child policy of Policy1. If Policy2 contains references to Policy3, the inventory views do not display Policy3 as a child of Policy1.

Attribute Name	Description
Management Mode	<p>Specifies whether the source node is managed or not</p> <p>Possible states are as follows:</p> <ul style="list-style-type: none"> • Managed: Indicates that the node is managed. • Not Managed: Indicates that the node is not managed on purpose. • Out of Service: Indicates that a node is unavailable because it is out of service.

The actions show one of the following threshold states:

Threshold States

State	Description
 High	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and this high value persists for the specified High Duration within the High Duration Window.</p>
 Nominal	Indicates that the measured value of the metric is within the normal healthy range.
 Unavailable	Unable to compute the metric or the computed value is outside the valid range.
 Threshold Not Set	Indicates that the threshold is not set for the metric.
 None	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero and this zero value persists for the specified duration within the High or Low Duration Window (depending on the metric).</p>

To open the QoS Action inventory view for an interface, select the interface and click  **Open**. For information about QoS Action inventory view, see "[Viewing QoS Actions Details](#)" on page 69.

You can filter the actions listed in this view based on all columns of this view.

If there are large number of QoS actions that crossed the threshold, you can filter those QoS actions based on the various QA groups. As you type, the auto-complete feature lists the matching QA Groups. You can select a QA Group name from the list.

Chapter 4: Accessing QA Group Details

Tip: For information about QA groups, see "[Configuring QA Groups](#)" on page 200

The QA Groups inventory view enables you to view the list of QA Groups that are configured in the network.

To launch the QA Groups Inventory View:

1. Log on to NNMi console using your user name and password.
2. Click **Quality Assurance** in the Workspaces panel.
3. Click **QA Groups**. The list of QA Groups with QA probes and QA Groups with QoS probes that are discovered in your network appear in the content pane along with some key attributes. By default, this information is refreshed every 300 seconds, or 5 minutes.

Key Attributes of the QA Groups Inventory View

The QA Groups Inventory view displays the following key attributes:

Attribute Name	Description
Group Name	The name of the QA group.
Group Type	The type of the QA group. The QA group type can be QA Probes, CBQoS, or Ping Latency.
Member count	The total number of entities that belong to the QA group. For more information, click here. <ul style="list-style-type: none">• For QA Probes: Total number of probes belonging to the group• For CBQoS: Total number of interfaces and actions belonging to the group• For Ping Latency: Total number of ping latency pairs belonging to the group
Tenant	Specifies the NNMi tenant for the QA Group.
Notes	Denotes any additional information, related to the QA group.

Viewing QA Group Details

The QA Groups form provides the details of the selected QA group. For QA Probes type of groups, this form also provides details about each QA probe that belongs to the group.

In the QA Group form of the QA Probes type, the following tabs are available:

- ["Probes" on the next page](#)
- [QA Groups Form: Probes Critical Tab](#)
- [QA Groups Form View: Probes Threshold Exception Tab](#)

- [QA Groups Form: Probes Baseline Exceptions Tab](#)
- [QA Groups Form: Registration Tab](#)

In the QA Group form of the QoS type, the following tabs are available:

- [QA Groups Form: QoS Interfaces Tab](#)
- [QA Groups Form: QoS Actions Tab](#)
- [QA Groups Form: QoS Interfaces Threshold Exceptions Tab](#)
- [QA Groups Form: QoS Actions Threshold Exceptions Tab](#)
- [QA Groups Form: Registration Tab](#)

In the QA Group form of the Ping Latency Pairs type, the following tabs are available:









- [QA Groups Form: Ping Latency Pairs Tab](#)
- [QA Groups Form: Registration Tab](#)













Probes

The **Probes** tab enables you to view the list of configured and discovered QA probes that belong to the QA group.










Key Attributes of the QA Groups- Probes Tab

The **probes** tab displays the following key attributes:

Attribute Name	Description
Status	<p>The status that the QA probe returned. NNM iSPI Performance for QA calculates the status based on the polling status of the nodes and the threshold states. A QA probe may return one of the following statuses:</p> <ul style="list-style-type: none"> •  Normal •  Warning •  Major •  Critical •  Unknown •  Disabled •  Not Polled •  No Status <p>For more information about status, see "Supported QA Probe Statuses" on page 45.</p>
Name	The name of the discovered QA probe configured in the network device.
Owner	The name of the discovered QA probe's owner.
Service	<p>The type of the discovered QA probe.</p> <p>Some of the QA probe types that the NNM iSPI Performance for QA recognizes are</p>

Attribute Name	Description
	as follows: <ul style="list-style-type: none"> • UDP Echo • ICMP Echo • UDP • TCP Connect • VoIP • HTTP • DNS • DHCP
Source	The source device in which the probe is configured.
Destination	The destination network device to which the probe is configured.
Source Site	The source site to which the configured probe is associated.
Destination Site	The destination site to which the configured probe is associated.
RTT	The round-trip time used by the selected QA probe. Displays one of the following threshold states for the metric: <ul style="list-style-type: none">  High  Nominal  Low  Not Polled  Unavailable  Threshold Not Set  None
Jitter	The delay ¹ variance for a data packet to reach the destination device or site. Displays one of the following threshold states for the metric: <ul style="list-style-type: none">  High  Nominal  Low  Not Polled  Unavailable

¹The time taken for a packet to travel from the sender network element to the receiver network element.

Attribute Name	Description
	 Threshold Not Set  None
PL (Packet Loss)	<p>The percentage of packets that failed to arrive at the destination.</p> <p>Displays one of the following threshold states for the metric:</p>  High  Nominal  Low  Not Polled  Unavailable  Threshold Not Set  None
Manager	Specifies whether the NNMi management server is Local or not. The name of the Regional Manager is displayed if the NNMi management server is not local.
Tenant	Specifies the NNMi tenant selected for the network device.

Critical Probes

The **Probes Critical** tab displays the list of critical QA probes that belong to the QA Group.

Attributes: Probes Critical Tab

The **probes critical** tab displays the following key attributes:




Attribute Name	Description
Operational State	<p>Operational State condition returned by the critical QA probe.</p> <p>The QA probe status is derived from the SNMP polling results for Operational State and from any conclusion.</p>
Administrative State	<p>Administrative State condition returned by the QA probe.</p> <p>The QA probe status is derived from the SNMP polling results for Administrative State and from any conclusion.</p>
Name	The name of the discovered QA probe configured in the network device.
Owner	The name of the discovered QA probe's owner.
Service	<p>The type of the discovered QA probe.</p> <p>Some of the QA probe types that the NNM iSPI Performance for QA recognizes are as follows:</p>


















Attribute Name	Description
	<ul style="list-style-type: none"> • UDP Echo • ICMP Echo • UDP • TCP Connect • VoIP • HTTP • DNS • DHCP • Oracle • HTTPS
Source	The source device from which the data packet is sent.
Source Tenant	Specifies the NMMi tenant selected for the network device.

Probes with Threshold Exceptions






















The **Probes Threshold Exception** tab enables you to view the QA Probes that belong to the QA Group, and have violated the threshold for one or more of the metrics.






















Key Attributes of the Probes Threshold Exception Tab:




Attribute Name	Description
Status	Displays the QA probes that are with the following status: <ul style="list-style-type: none"> •  Warning •  Major •  Critical
Name	The name of the discovered QA probe configured in the network device.
Service	The type of the discovered QA probe. Some of the QA probe types that the NMM iSPI Performance for QA recognizes are as follows: <ul style="list-style-type: none"> • UDP Echo • ICMP Echo • UDP • TCP Connect • VoIP • HTTP

Attribute Name	Description
	<ul style="list-style-type: none"> • DNS • DHCP
Manager	Specifies whether the NNMi management server is Local or not. The name of the Regional Manager is displayed if the NNMi management server is not local.
RTT	The round-trip time used by the selected QA probe. Displays any one of the following threshold states for the metric.  High  Nominal  Low  Not Polled  Unavailable  Threshold Not Set  None
Jitter	The delay ¹ variance for a data packet to reach the destination device or site. Displays one of the following threshold states for the metric:  High  Nominal  Low  Not Polled  Unavailable  Threshold Not Set  None
+ve Jitter SD	Indicates the threshold state of the positive jitter from the source to the destination. Displays one of the following threshold states for the metric:  High  Nominal  Low

¹The time taken for a packet to travel from the sender network element to the receiver network element.

Attribute Name	Description
	<p> Not Polled</p> <p> Unavailable</p> <p> Threshold Not Set</p> <p> None</p>
+ve Jitter DS	<p>Indicates the threshold state of the positive jitter from the destination to the source.</p> <p>Displays one of the following threshold states for the metric:</p> <p> High</p> <p> Nominal</p> <p> Low</p> <p> Not Polled</p> <p> Unavailable</p> <p> Threshold Not Set</p> <p> None</p>
-ve Jitter SD	<p>Indicates the threshold state of the negative jitter from the source to the destination.</p> <p>Displays one of the following threshold states for the metric:</p> <p> High</p> <p> Nominal</p> <p> Low</p> <p> Not Polled</p> <p> Unavailable</p> <p> Threshold Not Set</p> <p> None</p>
-ve Jitter DS	<p>Indicates the threshold state of the negative jitter from the destination to the source.</p> <p>Displays one of the following threshold states for the metric:</p> <p> High</p> <p> Nominal</p> <p> Low</p>

Attribute Name	Description
	 Not Polled  Unavailable  Threshold Not Set  None
PL (Packet Loss)	<p>The percentage of packets that failed to arrive at the destination.</p> <p>Displays one of the following threshold states for the metric:</p>  High  Nominal  Low  Not Polled  Unavailable  Threshold Not Set  None
Packet Loss SD	<p>Indicates the threshold state of the percentage of packet loss from the source to the destination.</p> <p>Displays one of the following threshold states for the metric:</p>  High  Nominal  Low  Not Polled  Unavailable  Threshold Not Set  None
Packet Loss DS	<p>Indicates the threshold state of the percentage of packet loss from the destination to source.</p> <p>Displays one of the following threshold states for the metric:</p>  High  Nominal  Low

Attribute Name	Description
	 Not Polled  Unavailable  Threshold Not Set
MOS	Indicates the threshold state of the Mean Opinion Score (MOS) of the jitter.
Source Tenant	Specifies the NNMi tenant selected for the network device.









Probes with Baseline Exceptions










The **Probes Baseline Exceptions** tab displays the list of QA probes that belong to the QA Group, and have the baseline state as Abnormal Range, Unavailable, No Policy, or Not Polled for one or more of the following metrics:
















- RTT
- Two Way Jitter
- Two Way Packet Loss
- MOS

Each probe displays information for a specific time interval.

Key Attributes of the Probes Baseline Exceptions tab

Attribute Name	Description
Status	Displays the QA probes that are with the following status: <ul style="list-style-type: none"> •  Normal •  Warning •  Major •  Critical •  Unknown •  Disabled •  Not Polled •  No Status For more information about probe status, see " Supported QA Probe Statuses " on page 45.
Name	The name of the discovered QA probe configured in the network device.
Service	The type of the discovered QA probe.

Attribute Name	Description
	<p>Some of the QA probe types that the NNM iSPI Performance for QA recognizes are as follows:</p> <ul style="list-style-type: none"> • UDP Echo • ICMP Echo • UDP • TCP Connect • VoIP • HTTP • DNS • DHCP
Manager	<p>Specifies whether the NNMi management server is Local or not. The name of the Regional Manager is displayed if the NNMi management server is not local.</p>
RTT	<p>The round-trip time used by the selected QA probe.</p> <p>Displays any one of the following baseline states for the metric:</p> <ul style="list-style-type: none"> •  Normal Range - The metric is within the normal range of deviation. •  Abnormal Range - The metric is above the configured normal range of the deviation. •  Unavailable - The computed value for the metric is not found in HP NNM iSPI Performance for Metrics Software. •  Unset - No baseline is computed. •  Not polled - The metric is not polled for baseline deviations. •  No Policy - No polling policy exists for this metric.
Two Way Jitter	<p>Indicates two way jitter. This value is the average of the following values:</p> <ul style="list-style-type: none"> • Positive jitter from the source to the destination • Negative jitter from the source to the destination • Positive jitter from the destination to the source • Negative jitter from the destination to the source <p>Displays one of the following baseline states for the metric:</p> <ul style="list-style-type: none"> •  Normal Range - The metric is within the normal range of deviation. •  Abnormal Range - The metric is either above or below the configured normal range of the deviation. •  Unavailable - The computed value for the metric is not found in HP NNM iSPI Performance for Metrics Software.

Attribute Name	Description
	<ul style="list-style-type: none"> •  Unset - No baseline is computed. •  Not polled - The metric is not polled for baseline deviations. •  No Policy - No polling policy exists for this metric.
Two Way Packet Loss	<p>The percentage of packets that failed to arrive from the source to destination and destination to source.</p> <p>Displays one of the following baseline states for the metric:</p> <ul style="list-style-type: none"> •  Normal Range - The metric is within the normal range of deviation. •  Abnormal Range - The metric is either above or below the configured normal range of the deviation. •  Unavailable - The computed value for the metric is not found in HP NNM iSPI Performance for Metrics Software. •  Unset - No baseline is computed. •  Not polled - The metric is not polled for baseline deviations. •  No Policy - No polling policy exists for this metric.
MOS	<p>Indicates the baseline state of the Mean Opinion Score (MOS) of the jitter.</p> <p>Displays one of the following baseline states for the metric:</p> <ul style="list-style-type: none"> •  Normal Range - The metric is within the normal range of deviation. •  Abnormal Range - The metric is either above or below the configured normal range of the deviation. •  Unavailable - The computed value for the metric is not found in HP NNM iSPI Performance for Metrics Software. •  Unset - No baseline is computed. •  Not polled - The metric is not polled for baseline deviations. •  No Policy - No polling policy exists for this metric.
Source Tenant	Specifies the NNMi tenant selected for the network device

Registration

The UUID attribute is valid for all object types. NNMi displays the ID and UUID attribute values on the object form's **Registration** tab:

- `{uuid}` Universally Unique Object Identifier - Unique across all databases.

For more information, see *NNMi Online Help for Administrators*

QoS Interfaces

The **QoS Interfaces** tab enables you to view the list of discovered QoS interfaces that belong to the group. The traffic can be ingress or egress for an interface. By default, this information is refreshed every 300 seconds, or 5 minutes.

The **QoS Interfaces** tab displays only the parent policies name, or only the policies name that are configured on the interfaces.

Key Attributes of the QoS Interfaces Tab

The **QoS Interfaces** tab displays the following key attributes:

Attribute Name	Description
Interface Name	The name of the interface.
Hosted on Node	The name of the node on which the interface resides.
In Policy	The name of the In policy ¹ associated with the interface.
Out Policy	The name of the Out policy ² associated with the interface.
Applied On	The interface on which the policy is applied. Possible values are: <ul style="list-style-type: none">Control PlaneInterface
Tenant	Specifies the NNMi tenant selected for the interface.
Management Server	Specifies whether the NNMi management server is Local or not. The name of the Regional Manager is displayed if the NNMi management server is not local.
Management Mode	Specifies whether the source node is managed or not. Possible states are as follows: <ul style="list-style-type: none">Managed: Indicates that the node is managed.Not Managed: Indicates that the node is not managed on purpose.Out of Service: Indicates that a node is unavailable because it is out of service.

QoS Actions

The **QoS Actions** tab enables you to view the list of [QoS Actions](#), which are applied to the QoS interfaces that belong to the QA Group, based on a particular traffic flow and a policy (Incoming and Outgoing traffic). By default, this information is refreshed every 300 seconds, or 5 minutes.

Key Attributes of the QoS Actions Tab

¹In Policy defines the policy which is applied to the incoming traffic.

²Out Policy defines the policy which is applied to the outgoing traffic.

The **QoS Actions** tab displays the following key attributes:

Attribute Name	Description
Action	The type of Action applied. Possible values are: <ul style="list-style-type: none">• Policing• Shaping• Queuing• Packet Marking• RED
Traffic Class Name	Name of the Traffic Class associated with the selected action.
Policy Name	The name of the policy applied. This attribute displays only the parent policies name, or the policies that are configured on the interfaces.
Direction	Indicates whether the policy was applied on the incoming traffic or outgoing traffic for an interface.
Interface Name	The name of the interface mapped to the QoS action.
Hosted On Node	The name of the node on which the interface resides.
Tenant	Specifies the NNMi tenant selected for the interface.
Management Server	Specifies whether the NNMi management server is Local or not. The name of the Regional Manager is displayed if the NNMi management server is not local.
Management Mode	Specifies whether the source node is managed or not. Possible states are as follows: <ul style="list-style-type: none">• Managed: Indicates that the node is managed.• Not Managed: Indicates that the node is not managed on purpose.• Out of Service: Indicates that a node is unavailable because it is out of service.

QoS Interfaces with Threshold Exceptions

The **QoS Interfaces Threshold Exceptions** tab enables you to view the list of QoS interfaces that belong to the QA Group, for which one of the following actions crossed the threshold and NNM iSPI Performance for QA raised an exception:

- Class State
- Packet Marking
- Policing
- Queuing

- Shaping
- RED


For information on each of the actions listed above, see [QoS Actions](#).

The **QoS Interfaces Threshold Exceptions** tab displays the following key attributes:





Attribute Name	Description
Interface Name	The name of interface.
Hosted on Node	The name of the node on which the interface resides.
Policy Name	The name of the policy applied on the selected interface. It displays only the parent policies name, or only the policies name that are configured on the interfaces.
Direction	Indicates whether the policy was applied on the incoming traffic or outgoing traffic for the selected interface.
Traffic Class Name	Name of an associated Traffic Class, based on a specific criterion.
Class State	Specifies the traffic class state.
Packet Marking	Specifies the threshold state for the "Packet Marking" action configured for one or more traffic classes associated with the selected policy.
Policing	Specifies the threshold state for the "Policing" action configured for one or more traffic classes associated with the selected policy.
Queuing	Specifies the threshold state for the "Queuing" action configured for one or more traffic classes associated with the selected policy.
Shaping	Specifies the threshold state for the "Shaping" action configured for one or more traffic classes associated with the selected policy.
RED	Specifies the threshold state for the "RED" action configured for one or more traffic classes associated with the selected policy.
Tenant	Specifies the NNMi tenant selected for the interface.

The actions shows one of the following threshold states:

Threshold States

State	Description
 High	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p>

Threshold States, continued




State	Description
	Indicates that the measured value of the metric is above the configured High Value and this high value persists for the specified High Duration within the High Duration Window.
 Nominal	Indicates that the measured value of the metric is within the normal healthy range.
 Unavailable	Unable to compute the metric or the computed value is outside the valid range.
 Threshold Not Set	Indicates that the threshold is not set for the metric.
 None	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero and this zero value persists for the specified duration within the High or Low Duration Window (depending on the metric).</p>













QoS Actions with Threshold Exceptions

The **QoS Actions Threshold Exceptions** tab enables you to view the list of QoS actions that crossed the threshold and NNM iSPI Performance for QA raised an exception.

For information about actions, see ["Quality of Service \(QoS\) Actions" on page 74](#).

The **QoS Actions Threshold Exceptions** tab displays the following key attributes:

Attribute Name	Description				
State	<p>The threshold state for the action.</p> <p>The actions shows one of the following threshold states:</p> <p>Threshold States</p> <table border="1"> <thead> <tr> <th>State</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td> High</td> <td> <p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> </td> </tr> </tbody> </table>	State	Description	 High	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p>
State	Description				
 High	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is above the configured High Value and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p>				

Attribute Name	Description												
	<p>Threshold States, continued</p> <table border="1" data-bbox="444 365 1377 1234"> <thead> <tr> <th data-bbox="444 365 685 424">State</th> <th data-bbox="685 365 1377 424">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="444 424 685 583"></td> <td data-bbox="685 424 1377 583">Indicates that the measured value of the metric is above the configured High Value and this high value persists for the specified High Duration within the High Duration Window.</td> </tr> <tr> <td data-bbox="444 583 685 676"> Nominal</td> <td data-bbox="685 583 1377 676">Indicates that the measured value of the metric is within the normal healthy range.</td> </tr> <tr> <td data-bbox="444 676 685 768"> Unavailable</td> <td data-bbox="685 676 1377 768">Unable to compute the metric or the computed value is outside the valid range.</td> </tr> <tr> <td data-bbox="444 768 685 861"> Threshold Not Set</td> <td data-bbox="685 768 1377 861">Indicates that the threshold is not set for the metric.</td> </tr> <tr> <td data-bbox="444 861 685 1234"> None</td> <td data-bbox="685 861 1377 1234"> <p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero and this zero value persists for the specified duration within the High or Low Duration Window (depending on the metric).</p> </td> </tr> </tbody> </table>	State	Description		Indicates that the measured value of the metric is above the configured High Value and this high value persists for the specified High Duration within the High Duration Window.	 Nominal	Indicates that the measured value of the metric is within the normal healthy range.	 Unavailable	Unable to compute the metric or the computed value is outside the valid range.	 Threshold Not Set	Indicates that the threshold is not set for the metric.	 None	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero and this zero value persists for the specified duration within the High or Low Duration Window (depending on the metric).</p>
State	Description												
	Indicates that the measured value of the metric is above the configured High Value and this high value persists for the specified High Duration within the High Duration Window.												
 Nominal	Indicates that the measured value of the metric is within the normal healthy range.												
 Unavailable	Unable to compute the metric or the computed value is outside the valid range.												
 Threshold Not Set	Indicates that the threshold is not set for the metric.												
 None	<p><i>For Count-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count.</p> <p><i>For Time-Based Threshold Configuration:</i></p> <p>Indicates that the measured value of the metric is zero and this zero value persists for the specified duration within the High or Low Duration Window (depending on the metric).</p>												
Action	The name of the action that crossed the threshold.												
Traffic Class Name	Name of the Traffic Class associated with the selected action.												
Policy Name	<p>The name of the policy associated with the selected action.</p> <p>This attribute displays only the parent policies name, or only the policies that are configured on the interfaces.</p>												
Direction	Indicates whether the policy was applied on the incoming traffic or outgoing traffic for an interface.												
Interface Name	The name of the interface associated with the selected action.												
Hosted on Node	The name of the node on which the interface resides.												
Tenant	Specifies the NNMi tenant selected for the interface.												
Management Server	Specifies whether the NNMi management server is Local or not. The name of the Regional Manager is displayed if the NNMi management server is not local.												









Attribute Name	Description
Management Mode	Specifies whether the source node is managed or not. Possible states are as follows: <ul style="list-style-type: none"> • Managed: Indicates that the node is managed. • Not Managed: Indicates that the node is not managed on purpose. • Out of Service: Indicates that a node is unavailable because it is out of service.

Ping Latency Pairs

The **Ping Latency Pairs** tab enables you to view the list of interfaces for which the Ping Latency Pairs are configured. By default, this information is refreshed every 300 seconds, or 5 minutes.

Key Attributes of the Ping Latency Pairs Tab

The **Ping Latency Pairs** tab displays the following key attributes:

Attribute Name	Description
Status	The status that the Ping Latency Pair returned. NNM iSPI Performance for QA calculates the status based on the polling status of the nodes and the threshold states. A Ping Latency Pair may return one of the following statuses : <ul style="list-style-type: none"> •  Normal •  Warning •  Major •  Critical •  Unknown •  Disabled •  Not Polled •  No Status For more information about status, see "Valid Ping Latency Pair Statuses " on page 53.
Name	The name of the discovered Ping Latency Pair configured in the network device.
Source	The source device on which the Ping Latency Pair is configured.
Source IfName	The name of the interface that triggers the ping request.
Source IP	IP address of the device on which the Ping Latency Pair probe is configured.

Attribute Name	Description
Destination	The destination device to which the Ping Latency Pair is configured.
Destination IfName	The name of the interface that receives the ping request.
Destination IP	The IP address of the destination device.
Tenant	Specifies the NNMi tenant selected for the interface.
Manager	Specifies whether the NNMi management server is Local or not. The name of the Regional Manager is displayed if the NNMi management server is not local.

Analysis Pane

Analysis Pane

The Analysis Pane of QA Groups shows the details of the selected QA Group (QA Probes, CBQoS, or Ping Latency Pair).

QA Probes

The analysis pane for QA Probes shows the details such as, QA Group summary, QA probes on QA groups, baseline state, and Threshold state.

QA Group Summary

The QA Group summary displays the following details about the QA Group and the probes that belong to the selected QA Group:

- Filter String
- Total number of probes
- Total number of normal probes
- Total number of disabled probes
- Total number of critical probes
- Total number of threshold exceeded probes
- Total number of baseline exceeded probes

QA Probes on QA Groups







This tab displays a pie-chart for the following QA Probes' status that belong to the selected QA Group:

-  Normal
-  Warning
-  Major
-  Critical
-  Unknown

-  Disabled
-  No Status







Baseline State

This tab displays a pie-chart for the following QA Probes' baseline threshold status that belong to the selected QA Group:

Threshold Status	Status indicating in the Pie-chart for the corresponding threshold status
Nominal, NOMINAL	 Normal
High, Low	 Major
Critical	 Critical
No status	 No Status
UNAVAILABLE, UNKNOWN	 Unknown
NOT POLLED, Not Polled, Threshold not set, Not defined	 Disabled

Threshold State

This tab displays a pie-chart for the following QA Probes' threshold status that belong to the selected QA Group:

Threshold Status	Status indicating in the Pie-chart for the corresponding threshold status
Nominal, NOMINAL	 Normal
High, Low	 Major
Critical	 Critical
No status	 No Status
UNAVAILABLE, UNKNOWN	 Unknown
NOT POLLED, Not Polled, Threshold not set, Not defined	 Disabled

CBQoS

The analysis pane for CBQoS QA Groups shows the details such as, QA Group summary, Threshold Exception Interfaces, and QoS Actions Threshold State.

QA Group Summary

The QA Group summary displays the following details about the QA Group and the probes that belong to the selected QA Group:

- Filter string
- Total number of CBQoS interfaces
- Total number of CBQoS Actions







Threshold Exception Interfaces

This tab displays the tabular representation of all CBQoS interfaces that belong to the QA Group, and with at least one of the metric thresholds violated.

Field Name	Description
Host Name	The host name of the node on which the interface is present.
Interface Name	Name of the interface.
Metric Name	The name of the metric.
Direction	Indicates whether the policy was applied on the incoming traffic or outgoing traffic for the selected interface.
Type	The type of threshold configured. Count-based or Time-based
High Value	The High Value indicates the high threshold value.
Rearm Value	The Rearm Value is used to indicate the end of the threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value.

QoS Actions Threshold State

This tab displays a pie-chart for the following QoS actions threshold states that belong to the QA Group:

Threshold Status	Status indicating in the Pie-chart for the corresponding threshold status
Nominal, NOMINAL	 Normal
High, Low	 Major
Critical	 Critical
No status	 No Status
UNAVAILABLE, UNKNOWN	 Unknown
NOT POLLED, Not Polled, Threshold not set, Not defined	 Disabled

Ping Latency Pair

The analysis pane for Ping Latency Pair QA Groups shows details such as, QA Group summary, and Ping Latency Pairs on QA Group.



QA Group Summary

The QA Group summary displays the following details about the QA Group and the Ping Latency Pairs that belong to the selected QA Group:

- Filter string
- Total number of Ping Latency Pairs

Ping Latency Pairs on QA Group

This tab displays a pie-chart for the following status of Ping Latency Pairs that belong to the QA Group:

-  Normal
-  Critical
-  No Status
-  Major

Viewing QA Probes Using Command Line Utilities

To display the QA probes associated with a QA group, use the following commands:

To display the QA Probes associated with a QA Group

QA Group Type	QA Group Command	Command Behavior
QA Probes		Displays the QA probes associated with the QA group
Linux	<code>\$NnmInstallDir/bin/nmsqacustomgrouputil.ovpl -u <username> -p <password> -display -gt QAProbes -g <QA group name></code>	
Windows	<code>%NnmInstallDir%\bin\nmsqacustomgrouputil.ovpl -u <username> -p <password> -display -gt QAProbes -g <QA group name></code>	
QoS		
Linux	<code>\$NnmInstallDir/bin/nmsqacustomgrouputil.ovpl -u <username> -p <password> -display -gt CBQOS -g <QA group name> -<interface or action for which the QA probe is configured></code>	
Windows	<code>%NnmInstallDir%\bin\nmsqacustomgrouputil.ovpl -u <username> -p <password> -display -gt CBQOS -g <QA group name> -<interface or action for which the QA probe is configured></code>	

To Save the QA Probes for the QA Group

QA Group Type	QA Group Command	Command Behavior
---------------	------------------	------------------

To Save the QA Probes for the QA Group, continued

QA Probes		Saves the QA Probes associated with the selected QA Group in a file. Provide absolute path for the file where you want to save the QA probes associated with the selected QA group.
Linux	<code>\$NnmInstallDir/bin/nmsqacustomgrouputil.ovpl -u <username> -p <password> -gt qaprobes -g <QA group name> -savetofile <filename></code>	
Windows	<code>%NnmInstallDir%\bin\nmsqacustomgrouputil.ovpl -u <username> -p <password> -gt qaprobes -g <QA group name> -savetofile <filename></code>	
QoS		
Linux	<code>\$NnmInstallDir/bin/nmsqacustomgrouputil.ovpl -u <username> -p <password> -gt CBQOS -g <custom group name> -<interface/action> -savetofile <filename></code>	
Windows	<code>%NnmInstallDir%\bin\nmsqacustomgrouputil.ovpl -u <username> -p <password> -gt CBQOS -g <custom group name> -<interface/action> -savetofile <filename></code>	

Note: -u <username> -p <password> are optional parameters.

Saving QA Probes Using Command Line Utilities

To save the QA probes associated with a QA group in a file, use the following commands:

To save the QA Probes for the QA Group

QA Group Type	QA Group Command	Command Behavior
---------------	------------------	------------------

To save the QA Probes for the QA Group, continued

QA Probes		Saves the QA Probes associated with the selected QA Group in a file. Provide absolute path for the file where you want to save the QA probes associated with the selected QA group.
Linux	<pre>\$NnmInstallDir/bin/nmsqacustomgrouputil.ovpl -u <username> -p <password> -gt qaprobes -g <QA group name> -savetofile <filename></pre>	
Windows	<pre>%NnmInstallDir%\bin\nmsqacustomgrouputil.ovpl -u <username> -p <password> -gt qaprobes -g <QA group name> -savetofile <filename></pre>	
QoS		
Linux	<pre>\$NnmInstallDir/bin/nmsqacustomgrouputil.ovpl -u <username> -p <password> -gt CBQOS -g <custom group name> -<interface/action> -savetofile <filename></pre>	
Windows	<pre>%NnmInstallDir%\bin\nmsqacustomgrouputil.ovpl -u <username> -p <password> -gt CBQOS -g <custom group name> -<interface/action> -savetofile <filename></pre>	

Note: -u <username> -p <password> are optional parameters.

Chapter 5: Monitoring Using Maps

The NNM iSPI Performance for QA provides you with the following maps:

Site Map: Site Map enables you to monitor the performance of a site and gives a holistic view of the network. For more information about site maps, see ["Using Site Map " on the next page](#)

Node Response View: This map enables you to monitor the performance of each node that builds your network by providing a comprehensive overview of the selected node's health and performance. For more information about Node Response View, see ["Using Node Response View" on page 111](#).

Global Node Response View: This map enables you to view the status of all the discovered nodes and provides you with a comprehensive overview of the network health and performance. For more information about Global Node Response View, see [" Using Global Node Response View" on page 115](#)

QoS Map: This map enables you to monitor the nodes and interfaces that are QoS enabled. For more information about QoS Maps, see ["Using QoS Maps" on page 119](#).

Using Site Map

You can view the performance of a network in a QA probe inventory view or form view. In a large enterprise network, Site Map enables you to easily identify, assess, and monitor the performance of any site and give a holistic view of the network.

The site map represents the [sites](#)¹ as nodes, and the most severe probe status as links between the sites.

The following table lists the terminologies used in site map:



Terminology	Description
Site Status	<p>Links are unidirectional for the QA probes originating from the source to destination site. The color of the link is based on the threshold state of the probe for the selected service and metric.</p> <p>In the case of a two-way jitter, the link color is based on the threshold state of the metric in the source, and destination sites.</p>
Links	<p>Links are unidirectional for the QA probes originating from the source to destination site. The color of the link is based on the threshold state of the probe for the selected service and metric.</p> <p>In the case of a two-way jitter, the link color is based on the threshold state of the metric in the source, and destination sites</p>

You can retrieve the data from NNM iSPI Performance for QA, and you can view the site map in the NNMI console.




You can view the site map only if you have the permission to access at least one QA probe in the site.

Site status and the overall view of the site map varies based on your access to a set of probes in a site. If you have access to a set of probes in a site, the site status appears based on the overall status of those probes in a site.

The following table shows the coloring scheme for the site status or the QA probe status:





Status Color	Status Description
	No Status/Disabled/Warning
	Normal

¹A logical organization of networking devices. In the scope of enterprise networks, a site can be a logical grouping of networking devices generally situated in similar geographic location. The location can include a floor, building or an entire branch office or several branch offices which connect to head quarters or another branch office via WAN/MAN. Each site is uniquely identified by its name. In case of the service provider networks the Virtual Routing and Forwarding (VRF) on a Provider Edge (PE) router or a Customer Edge (CE) routers can be defined as a site.

Status Color	Status Description
	Unknown
	Major
	Critical

If there are no probes configured in a destination site, the site status displays in Gray color indicating - No Status. However, if there are no probes configured from the source to the destination site, no link appears between the source and the destination site.


The following table shows the coloring scheme of the link or the Threshold state:

Link Color	Threshold State Description
	High
	Nominal
	Low Applicable only for the Mean Opinion Score (MOS) metric of the VoIP service
	Threshold Not Set / Undefined / Not Polled / No Polling Policy

You can double-click on the link in the site map to view the QA Probe summary details in the Analysis pane. In addition, you can double-click on the site to get a form view of all the QA Probes originating from the site.

Launching the Site Map




To launch the site map, follow these steps:

1. Log on to NNMi console using your user name and password.
2. Select **Actions** → **Quality Assurance** → **Site Map** from the NNMi console to view the site map.
3. Select the service from the **Service** drop-down list. By default, NNM iSPI Performance for QApopulates the ICMP Echo service. See the table below for more information.
4. Select the metric from the **Metric** drop-down list. By default, NNM iSPI Performance for QApopulates the RTT metric name. See the table below for more information.
5. Optionally, type the site or search string of the sites for which you intend to view the site map in the **Site Selection** box.
6. Click  **Launch** to launch the site map for the selected service and metric.

The site map displays the source site if the destination site is not configured. The site map appears only if there are probes configured in the source site.




The site map automatically refreshes every five minutes.

You can perform the following tasks using the Site Map page:

Icons	Description
 Open	Opens the selected site details.
 Refresh	Refreshes the view, site status ¹ and link status ² in the site map.
 Refresh Status	Refreshes only the site status in the site map.
Service <input type="text" value="ICMP Echo"/> Service	Select one of the following Services from the drop-down list for which you intend to view the site map: <ul style="list-style-type: none"> • UDP Echo • ICMP Echo • UDP • TCP Connect • VoIP • HTTP • DNS • HTTPS • Oracle • DHCP By default, NNM iSPI Performance for QA populates the ICMP Echo Service.
Metric <input type="text" value="RTT"/> Metric	Select any one of the following metrics from the drop-down list for which you intend to view the site map: <ul style="list-style-type: none"> • RTT • +ve Jitter • -ve Jitter • TwoWay Packet Loss • TwoWay Jitter • MOS By default, NNM iSPI Performance for QA populates the RTT Metric Type. +ve and -ve Jitter are always from source to

¹The status and coloring scheme of the map component is derived based on the most severe operational status of all the QA probes originating from the source map component for the selected service, and metric. A map component can be a site in Site Map or node in Node Map.

²Links are unidirectional for the QA probes originating from the source to the destination node. The color of the link is based on the threshold state of the probe for the selected service and metric.

Icons	Description
	destination in the site map. +ve Jitter, -ve Jitter, and Two-Way Jitter metrics are applicable only for UDP and VoIP service. The Mean Opinion Score (MOS) metric is applicable only for VoIP service.
Site Selection <input type="text"/> Site Selection	Type the name of the site or the search string of the sites, and click  to view a specific set of sites in the site map. You can enter the site name partially with the wild card asterisk "*" (to replace any number of characters) to retrieve all the sites based on the search string. For example, if you want to view all the sites starting with Ban, enter Ban* in the search string. Also, you can use the wild card "?" to replace one character in the search string. For example, if you want to view the sites starting with any one character followed by the string test_site, enter ?test_site in the search string. You can also use a combination of the wildcard * and ? in the search string. This search for the sites is case-sensitive .
 Launch	Launches the site map based on the selection. The site map also launches for the sites that have no destination sites.
 Find	Displays a drop-down list from where you can select the site that you want to find in the site map.

The site map displays a message if you select a wrong combination of the service and metric. For example, if you select ICMP Echo and +ve Jitter metric, a message appears indicating that the +ve Jitter metric is valid for UDP or VoIP Service.

If some QA probes in a site are disabled and others are of Nominal status, the Site map displays the Site status as Nominal. While displaying the color of the Site Status, the QA probes of Disabled status has lesser priority compared to Normal QA probe status.

Analysis Pane

Select the site by clicking the site in the site map to view the Analysis pane of the selected site. You can view the summary of the selected site. Additionally, you can view the pie charts of the Destination Site Probe Status Distribution in percentage, and Source Site Probe Status Distribution in percentage by clicking the respective tabs.

The Site status displays the overall status of all probes from the source node.

Using Node Response View

The Node Response View enables you to assess the performance of each node that builds your network. It displays a map that provides you with a comprehensive overview of the selected node's health and performance. This enables you to understand and monitor the performance of your network on a more granular level.

The map displays the status of the nodes available in the network for the selected filter criteria. The links between the nodes reflect the status of the probes running between the nodes.

NNM iSPI Performance for QA displays the link as a thick line if multiple (more than five) QA probes of the same probe type runs between the source node and destination node. The thick line displays the combined status of the all the probes running between the source and destination nodes.

Note: You can double-click the thick line to view the individual probes configured.

By default, the Node Response View is refreshed every five minutes. This refresh includes status change of all the map objects currently displayed.





Note: Node Response View can be launched successfully for a maximum of 500 probes.


The following table lists the terminologies used in the Node Response View:

Terminology	Description
Node Status	The status and coloring scheme of a node is derived based on the node status as displayed in NNMi.
Links	The status and coloring scheme of the links is based on the probe status (probes failure or probes exceeding threshold).









The node status and the Node Response View depends on your access to a set of probes originating from a selected node. The node status and Node Response View can be different for another user depending on the QA probes that they can access.

The following table lists the coloring scheme for the link status:

Color	Meaning	Description
	Disabled	Indicates the probe is disabled temporarily.
	Normal	Indicates the probe is running and the destination is reachable.
	Unknown	NNM iSPI Performance for QA displays the link status as Unknown for the following reasons: <ul style="list-style-type: none">• Source node is not reachable from NNMi.• Any of the probe's metric threshold state is not computed yet.
	Major	Indicates the probe has violated the threshold configured for the selected metric.

Color	Meaning	Description
	Critical	Indicates the destination node or interface is not reachable.

The following table lists the coloring scheme for the link status if there are multiple (more than five) probes configured between the source and destination nodes:


Color	Meaning	Description
	Unknown	Indicates that all probes configured between the source and destination nodes have a status of Unknown.
	Normal	Indicates that all probes configured between the source and destination nodes have a status of Normal.
	Minor	Indicates all probes but one from the multiple probes configured between the source and destination nodes have a status of Normal. The status of one probe is Minor, Warning, or Critical.
	Warning	Indicates one of the following: <ul style="list-style-type: none"> All probes configured between the source and destination nodes have a status of Warning. All probes configured between the source and destination nodes do not have the same status and none of the probes configured between the source and destination nodes have a status of Major or Minor.
	Major	Indicates all probes but one from the multiple probes configured between the source and destination nodes have a status of Critical. One probe has a status of either Normal, Warning, Minor, or Major.
	Critical	Indicates that all probes configured between the source and destination nodes have a status of Critical.
	Disabled	Indicates that all probes configured between the source and destination nodes have a status of Disabled.
	No status	Indicates that all probes configured between the source and destination nodes have a status of No Status.

You can click the link in the Node Response View to view the QA Probe summary details in the Analysis pane. Additionally, you can double-click a node to get a form view of all the QA Probes originating from the node.

Launching the Node Response View




To launch the Node Response View, follow these steps:

1. Log on to NNMi console using your user name and password.
2. Select one or more nodes.
3. Select **Actions** → **Quality Assurance** → **Node Response View** from the NNMi console to view the Node Response View.

4. Select the type of the view from the **Type** list.
5. Select the service from the **Service** list. By default, NNM iSPI Performance for QA displays the ICMP Echo service.
6. Select the metric from the **Metric** list. By default, NNM iSPI Performance for QA displays the Availability metric.
7. Select the type of exception raised on the selected metric in the Exception Mode list.
8. *Optional.* Type the source or destination node in the **Source** and **Destination** box.
 HP recommends that you specify the source or destination node to display meaningful information in the Node Response View.
 The response view appears only if there are probes configured in the source node.
9. Click  **Launch** to launch the Node Response View for the selected filter criteria.

The Node Response View automatically refreshes every five minutes.

You can perform the following tasks using the Node Response View form:

Icons	Description
 Open	Opens the selected node details.
 Refresh	Refreshes the view, node status ¹ and link status ² in the Node Response View.
 Refresh Status	Refreshes only the node status in the Node Response View.
Type	Select one of the following options: <ul style="list-style-type: none"> • Between³ • Source Centric⁴ • Destination Centric⁵
Service	Select one of the following Services from the drop-down list: <ul style="list-style-type: none"> • DNS



¹The status and coloring scheme of the map component is derived based on the most severe operational status of all the QA probes originating from the source map component for the selected service, and metric. A map component can be a site in Site Map or node in Node Map.

²Links are unidirectional for the QA probes originating from the source to the destination node. The color of the link is based on the threshold state of the probe for the selected service and metric.

³ Enables the Node Response View to display bi-directional links between the selected source and destination nodes.

⁴ Enables the Node Response View to display links from the selected source node and all the destination nodes. This is the default selection.

⁵ Enables the Node Response View to display links between the selected destination node and the source node.

Icons	Description
	<ul style="list-style-type: none"> • HTTP • HTTPS • ICMP Echo (Default) • ORACLE • TCP Connect • UDP Echo • UDP Jitter • VoIP
Metric	<p>Select one of the following metrics:</p> <ul style="list-style-type: none"> • + ve Jitter • -ve Jitter • Availability (Default) • MOS • RTT • Two Way Jitter • Two Way Packet Loss <div style="background-color: #f0f0f0; padding: 5px;"> <ul style="list-style-type: none"> • +ve and -ve Jitter always apply from source node to destination node • +ve Jitter, -ve Jitter, and Two Way Jitter metrics are applicable only for UDP and VoIP services. • Mean Opinion Score (MOS) metric is applicable only for the VoIP service. </div>
 Launch	Launches the Node Response View based on the selection.
 Find	Displays a drop-down list, from where you can select the node that you want to find in the Node Response View.

If some QA probes configured for a node are disabled and others are of Nominal status, the Node Response View displays the node status as Nominal. While displaying the color of the Node Status, the QA probes of Disabled status has lesser priority compared to Normal QA probe status.

Select the node by clicking the node in the Node Response View to view the Analysis pane of the selected node. The Analysis pane displays the summary and the detailed information of the selected node.

The node status displays the overall status of all probes from the source node.

Using Global Node Response View

Global Node Response View enables you to view the status of all the discovered nodes and provides you with a comprehensive overview of the network health and performance.

The Global Node Response View represents all nodes available in the network. You can select a source node or destination node and filter the view to display the status of the selected nodes.

The links between the nodes reflect the status of the probes running between the nodes.

Note: Global Node Response View can be launched successfully for a maximum of 500 probes.

By default, the Global Node Response View is refreshed every five minutes. This refresh includes status change of all the map objects currently displayed.




The following table lists the terminologies used in the Global Node Response View:



Terminology	Description
Node Status	The status and coloring scheme of a node is derived based on the node status as displayed in NNMi.
Links	<p>The status and coloring scheme of the links is based on the probe status (probes failure or probes exceeding threshold).</p> <p>NNM iSPI Performance for QA displays the link as a thick line if multiple (more than five) QA probes of the same probe type runs between the source node and destination node. The thick line displays the combined status of the all the probes running between the source and destination nodes.</p> <p>Note: You can double-click the thick line to view the individual probes configured.</p>

The node status and the Global Node Response View depends on your access to a set of probes originating from a node.









The node status and Global Node Response View can be different for another user depending on the QA probes that they can access.

The following table lists the coloring scheme for the link status in a Global Node Response View:

Color	Meaning	Description
	Disabled	Indicates the probe is disabled temporarily.
	Normal	Indicates the probe is running and the destination is reachable.
	Unknown	<p>NNM iSPI Performance for QA displays the link status as Unknown for the following reasons:</p> <ul style="list-style-type: none">• Source node is not reachable from NNMi.

Color	Meaning	Description
		<ul style="list-style-type: none"> Any of the probe's metric threshold state is not computed yet.
	Major	Indicates the probe has violated the threshold configured for the selected metric.
	Critical	Indicates the destination node or interface is not reachable.


The following table lists the coloring scheme for the link status if there are multiple (more than five) probes configured between the source and destination nodes:

Color	Meaning	Description
	Unknown	Indicates that all probes configured between the source and destination nodes have a status of Unknown.
	Normal	Indicates that all probes configured between the source and destination nodes have a status of Normal.
	Minor	Indicates all probes but one from the multiple probes configured between the source and destination nodes have a status of Normal. The status of one probe is Minor, Warning, or Critical.
	Warning	Indicates one of the following: <ul style="list-style-type: none"> All probes configured between the source and destination nodes have a status of Warning. All probes configured between the source and destination nodes do not have the same status and none of the probes configured between the source and destination nodes have a status of Major or Minor.
	Major	Indicates all probes but one from the multiple probes configured between the source and destination nodes have a status of Critical. One probe has a status of either Normal, Warning, Minor, or Major.
	Critical	Indicates that all probes configured between the source and destination nodes have a status of Critical.
	Disabled	Indicates that all probes configured between the source and destination nodes have a status of Disabled.
	No status	Indicates that all probes configured between the source and destination nodes have a status of No Status.

You can click the link in the Global Node Response View to view the QA Probe summary details in the Analysis pane. Additionally, you can double-click on the node to get a form view of all the QA Probes originating from the node.




Launching the Global Node Response View

To launch the Global Node Response View, follow these steps:

1. Log on to NNMi console using your user name and password.
2. Select **Actions** → **Quality Assurance** → **Global Node Response View** from the NNMi console to view the Global Node Response View.
3. Select the type of the view from the **Type** list.
4. Select the service from the **Service** list. By default, NNM iSPI Performance for QA displays the ICMP Echo service.
5. Select the metric from the **Metric** list. By default, NNM iSPI Performance for QA displays the Availability metric.
6. Select the type of exception raised on the selected metric from the Exception Mode list.
7. *Optional.* Type the source or destination node in the **Source** and **Destination** box.
 The response view appears only if there are probes configured in the source node.
8. Click  **Launch** to launch the Global Node Response View for the selected filter criteria.

The Global Node Response View automatically refreshes every five minutes.

You can perform the following tasks using the Global Node Response View form:

Icons	Description
 Open	Opens the selected node details.
 Refresh	Refreshes the view, node status ¹ and link status ² in the Global Node Response View.
 Refresh Status	Refreshes only the node status in the Global Node Response View.
Type	Select one of the following options: <ul style="list-style-type: none"> • Between³ • Source Centric⁴ • Destination Centric⁵
Service	Select one of the following Services from the drop-down list:



¹The status and coloring scheme of the map component is derived based on the most severe operational status of all the QA probes originating from the source map component for the selected service, and metric. A map component can be a site in Site Map or node in Node Map.

²Links are unidirectional for the QA probes originating from the source to the destination node. The color of the link is based on the threshold state of the probe for the selected service and metric.

³ Enables the Global Node Response View to display bi-directional links between the selected source and destination nodes.

⁴ Enables the Global Node Response View to display links from the selected source node and all the destination nodes. This is the default selection.

⁵ Enables the Global Node Response View to display links between the selected destination node and the source node.

Icons	Description
	<ul style="list-style-type: none"> • DNS • HTTP • HTTPS • ICMP Echo (Default) • Oracle • TCP Connect • UDP Echo • UDP Jitter • VoIP • DHCP
Metric	<p>Select one of the following metrics:</p> <ul style="list-style-type: none"> • + ve Jitter • -ve Jitter • Availability (Default) • MOS • RTT • Two Way Jitter • Two Way Packet Loss <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <ul style="list-style-type: none"> • +ve and -ve Jitter always apply from source node to destination node. • +ve Jitter, -ve Jitter, and Two Way Jitter metrics are applicable only for UDP and VoIP services. • Mean Opinion Score (MOS) metric is applicable only for the VoIP service. </div>
 Launch	Launches the Global Node Response View based on the selection.
 Find	Displays a drop-down list, from where you can select the node that you want to find in the Global Node Response View.

If some QA probes configured for a node are disabled and others are of Nominal status, the Global Node Response View displays the node status as Nominal. While displaying the color of the Node Status, the QA probes of Disabled status has lesser priority compared to Normal QA probe status.

Select the node by clicking the node in the Global Node Response View to view the Analysis pane of the selected node. The Analysis pane displays the summary and the detailed information of the selected node.

The node status displays the overall status of all probes from the source node.

Using QoS Maps

NNM iSPI Performance for Quality Assurance Software enables you to monitor the nodes and interfaces that are QoS enabled, using the QoS Maps feature. The map displays the set of nodes and interfaces that satisfies the specific filter criteria.

A node that does not have any QoS enabled interface is shown in gray. If an interface in the QoS map is not QoS enabled, it is also shown in gray.

Note: QoS map can be launched successfully for a maximum of 1000 interfaces.

Following are the types of QoS Maps that can be launched to monitor the QoS enabled interfaces:

- **QA Group QoS Map:** You can view the QoS enabled nodes that belong to the QA group and satisfy the filter criteria. The nodes are displayed with their first hop neighbor.
- **QoS Neighbor Map:** You can view the selected QoS enabled node or interface, and its first hop neighbor.

QA Group QoS Map

To launch the QA Group QoS map, follow these steps:




1. Log on to NNMi console using your user name and password.
2. Select **Quality Assurance** → **QA Groups**.
3. Select a QA Group and select **Actions** → **Quality Assurance** → **QoS Map**.











Nodes and interfaces in the QoS map can be filtered based on Traffic Class Name, Action, and Hop Count. Selecting a value from the drop-down list for any of the parameters automatically refreshes the map view and displays the set of nodes and interfaces that meets the selected filter criteria.


The status and coloring scheme of the interface is derived from the most severe of all threshold states configured on the interface.

The status and coloring scheme of the interface link is derived from the most severe threshold state of the bandwidth utilization metric on either interface of the link. The link color changes whenever there is a change in the threshold state.

The Quality Assurance QoS Map view toolbar lets you perform the following tasks within the displayed map:

Icon	Description
 Open	Opens the selected node details.
 Refresh	Refreshes the topology.
 Fit Content	Adjusts the size of the node symbols so that all members of the Node Group fit within the current window.

Icon	Description
 Actual Size	Cancels any current zoom setting.
 Zoom Out	Zooms out 25% of current size.
 Zoom In	Zooms in 25% of current size.
 Close	Closes the current view.
Traffic Class Name  Traffic Class Name	Select one of the traffic class names from the drop-down list for which you intend to view the QoS Map. By default, there is no traffic class name selected.
Action  Action	Select one of the following actions from the drop-down list for which you intend to view the QoS Map: <ul style="list-style-type: none"> • Packet Marking • Police • Queuing • RED • Shape By default, there is no action selected.
Hop Count  Hop Count	Displays the number of QoS hop neighbors that you want to view. By default, NNM iSPI Performance for QA populates the hop count as 1.
 Find	Displays a drop-down list where you can select the node that you want to find in the QoS Map.
 Tool Tips	Toggles on or off Tool Tips information that pops up when the mouse cursor is placed over an object on a map.
 Overview Location	Toggles on or off Overview Pane location. You can choose which corner of the map contains the Overview Pane or hide the Overview Pane. To set the Overview Pane location, toggle the Overview Location button on and from the menu, select the location you want.





Note: You cannot refresh the status of the node, interfaces and links in the QoS Map using the  **Refresh Status** icon. By default, the QoS Map is refreshed every five minutes. This refresh includes a full topology refresh of the map. The status of all nodes, interfaces and interface links are refreshed along with any changes in the topology.

Analysis Pane




Select the QoS-enabled node by clicking the node in the QoS map to view the Analysis pane of the selected node. You can view the summary of the selected node. In addition, you can view the Node Component Gauges, MIB Values, Status History, State Poller details, Security information, and Layer 2 Map, by clicking the respective tabs.

Select an interface on the QoS-enabled node in the QoS map to view the Analysis pane of the selected interface. You can view the QoS Interface Summary. In addition, you can view the Threshold State and Traffic Classes associated with the selected node by clicking the respective tabs.

QoS Interface Status

-  Threshold not set, Not defined - No threshold is configured on the QoS interfaces.
-  No status - The interface is not QoS enabled or it does not satisfy the filter criteria. For example, an interface may be QoS enabled but does not have the traffic class on which the filter is applied.
-  Major - At least one of the threshold states configured on the interface is breached for the QoS metric.
-  Normal - The threshold state of the QoS metric configured on the interface is within the defined threshold.

QoS Interface Link Status

-  Threshold not set, Not defined - Queue Bandwidth Utilization threshold is not configured on both ends of the link.
-  Major - At least one of the Queue Bandwidth Utilization threshold states configured on the link has breached the threshold.
-  Normal - There are no Queue Bandwidth Utilization threshold violations on both ends of the link.

QoS Neighbor Map

To launch the QoS Neighbor Map, follow these steps:

1. Log on to NNMi console using your user name and password.
2. You can launch the QoS Neighbor Map by selecting a QoS-enabled node from the NNMi Node Inventory, NNMi Network Overview map, QoS Interface Inventory, or QoS Interface Threshold Exceptions Inventory. If a node is not QoS enabled, the QoS Neighbor Map option is disabled.

To launch from the NNMi Node Inventory:

- a. Click **Inventory** → **Nodes**.
- b. Select a node and go to step 3.

To launch from the NNMi Network Overview:

- a. Click **Topology Maps** → **Network Overview**.
- b. Select a node and go to step 3.

To launch from the QoS Interfaces Inventory:

- a. Click **Quality Assurance** → **QoS Interfaces**.
- b. Select an interface and go to step 3.

To launch from the QoS Interfaces Threshold Exception Inventory:

- a. Click **Quality Assurance** → **QoS Interfaces Threshold Exceptions**.
- b. Select an interface and go to step 3.









3. Select **Actions** → **Quality Assurance** → **QoS Neighbor Map**.






QoS neighbor map shows the selected node and its first hop neighbor with its QoS information. If the selected node has more than one QoS enabled interfaces, it shows the first hop neighbor for each of the QoS enabled interfaces.


By default, the QoS Neighbor Map is refreshed every five minutes. This refresh includes status change of all the map objects currently displayed.

Nodes and interfaces displayed on the QoS Neighbor Map can be filtered based Traffic Class Name, Action, and Hop Count. Selecting a value from the drop-down list for any of the parameters automatically refreshes the map view and displays the set of nodes and interfaces that meets the selected filter criteria.

The Quality Assurance QoS Neighbor Map view toolbar lets you perform the following tasks within the displayed map:

Icon	Description
 Open	Opens the selected node details.
 Refresh	Refreshes the topology.
 Fit Content	Adjusts the size of the node symbols so that all members of the Node Group fit within the current window.
 Actual Size	Cancels any current zoom setting.
 Zoom Out	Zooms out 25% of current size.
 Zoom In	Zooms in 25% of current size.
 Close	Closes the current view.
Traffic Class Name  Traffic Class Name	Select one of the traffic class names from the drop-down list for which you intend to view the QoS Neighbor Map. By default, there is no traffic class name selected.

Icon	Description
 Action	Select one of the following actions from the drop-down list for which you intend to view the QoS Neighbor Map: <ul style="list-style-type: none"> • Packet Marking • Police • Queuing • RED • Shape By default, there is no action selected.
 Hop Count	Displays the number of QoS hop neighbors that you want to view. By default, NNM iSPI Performance for QA populates the hop count as 1.
 Find	Displays a drop-down list where you can select the node that you want to find in the QoS Neighbor Map.
 Tool Tips	Toggles on or off Tool Tips information that pops up when the mouse cursor is placed over an object on a map.
 Overview Location	Toggles on or off Overview Pane location. You can choose which corner of the map contains the Overview Pane or hide the Overview Pane. To set the Overview Pane location, toggle the Overview Location button on and from the menu, select the location you want.

Note: You cannot refresh the status of the node, interfaces and links in the QoS Neighbor Map using the  **Refresh Status** icon. By default, the QoS Neighbor Map is refreshed every five minutes. This refresh includes a full topology refresh of the map. The status of all nodes, interfaces and interface links are refreshed along with any changes in the topology.

Analysis Pane

Select the QoS-enabled node by clicking the node in the QoS neighbor map to view the Analysis pane of the selected node. You can view the summary of the selected node. In addition, you can view the Node Component Gauges, MIB Values, Status History, State Poller details, Security information, Layer 2 Map, and QA Probes (Node as Source), by clicking the respective tabs. When you select the QA Probes (Node as Source) tab, you can view the status of the probes that have the selected node as the source node.

Chapter 6: Monitoring Using Graphs

The Real Time Line graph enables you to do the following tasks :

- View the graph based on the real-time data of the metrics
- View the graph for QA probes configured on a node
- View the graph for selected QA probes
- View the trend of the selected metric value, and analyze the performance based on the metric values at polling intervals

The NNM iSPI Performance for QA supports Multi-Tenancy architecture configured in NNMi. A user can view the Real Time Line graph only if the source node or QA probe can be accessed by the user.

You can view a toolbar in the Real Time Line graph. See *Using Line Graphs* topic in the *HP Network Node Manager i Software Online Help* for information about the toolbar.

For more information about Real Time Line graphs, see "[Launching Real Time Line Graphs](#)" below.

Launching Real Time Line Graphs

Perform the following steps to launch a Real Time Line graph:

1. Log on to NNMi console using your user name and password.
2. You can either launch the graph for the QA probes configured on the node, or you can launch the graph for selected QA probes from one of the following Inventory views:
 - QA Probes View
 - Critical Probes View
 - Threshold Exceptions Probes View
 - Baseline Exceptions Probes View
3. To launch the graph for QA probes configured on a node, follow these steps:
 - a. Click **Inventory** in the Workspaces panel.
The **Inventory** tab expands.
 - b. Click **Nodes**, and the Node view appears.
Select the node for which you need to view the Real Time Line graph.
 - c. Select **Actions** → **Quality Assurance** → **Graph** → **<Service>** → **<metric name>** → **<metric sub menu>**
4. Alternatively, to launch the graph for selected QA probes, follow these steps:
 - a. Click **Quality Assurance** in the Workspaces panel. The Quality Assurance tab expands, displaying the **QA Probes** view.
 - b. Select the QA probes for which you require to view the Real Time Line graph.
 - c. Select **Actions** → **Quality Assurance** → **Graphs** → **<metric name>** → **<metric sub menu>**

If a node has numerous probes configured, it is recommended you launch the Real Time Line graph for selected probes rather than launching the Real Time Line graph for a node. This facilitates you to make use of the Real Time Line graph effectively.

5. The following table lists the valid **service**, **metric name** and the **metric sub menu**:

Service	Metric Name	Metric Sub Menu
UDP or TCP or VoIP	Jitter	<ul style="list-style-type: none"> • Mean Opinion Score • Negative Jitter DS • Negative Jitter SD • Positive Jitter DS • Positive Jitter SD • Two Way Jitter
	Packet Loss	<ul style="list-style-type: none"> • Percentage Packet Loss DS • Percentage Packet Loss SD • Two Way Packet Loss %
	Round Trip Time	<ul style="list-style-type: none"> • RTT in Milliseconds • RTT in Microseconds
ICMP Echo	Round Trip Time	<ul style="list-style-type: none"> • RTT in Milliseconds • RTT in Microseconds
UDP Echo	Round Trip Time	<ul style="list-style-type: none"> • RTT in Milliseconds • RTT in Microseconds
HTTP or HTTP(S)	Round Trip Time	<ul style="list-style-type: none"> • RTT in Milliseconds • RTT in Microseconds
DHCP	Round Trip Time	<ul style="list-style-type: none"> • RTT in Milliseconds • RTT in Microseconds
DNS	Round Trip Time	<ul style="list-style-type: none"> • RTT in Milliseconds • RTT in Microseconds

The Real Time Line Graph appears. In a Global Network Management environment, you cannot view the Real Time Line graph for the [Remote QA Probes](#)¹.

Also, you can view the Real Time Line graph only for the metrics supported by the vendor-specific devices.

All the metrics of NNM iSPI Performance for QA are supported by Cisco devices.

The Juniper RPM devices supports the following metrics:

- Negative Jitter DS
- Negative Jitter SD
- Positive Jitter DS
- Positive Jitter SD
- Two Way Packet Loss
- RTT in Milliseconds

The other devices supporting the DISMAN-PING using RFC 4560 supports only the RTT Milliseconds metric.

An error message appears if you select a metric not supported by the vendor device.

6. You can view a tool bar in the Real Time Line Graph, which facilitates you to traverse and extensively use the graph. The tool bar has the following menus and sub-menus:

Menu	Sub-Menu	Description
File	Select Lines...	Select lines in the real time line graph.
	Export to CSV	Export the real time line graph to a csv file.
	Print...	Print the real time line graph.
View	Legend	View the legend for the real time line graph.
	Time Line Viewer	Highlight a section of the data in the graph and continue to display all the data available.
	Lock Y-Axis	Lock or unlock the Y-axis while viewing time segments of the graph.
	Notification History	View the notification history in a pop up window.
Help	Graph Data Description	Get help on the graph data description.
	Using Line Graphs	Get help on using line graphs.

¹At Global server, the probes discovered and forwarded by regional servers are called as remote probes. You can manage threshold for these probes only at regional manager.

See *Using Line Graphs* topic in the *HP Network Node Manager Online Help* for more information on the toolbar menus, sub-menus, zoom factor, timeline viewer, and any other details pertaining to the graph.

7. You can select the polling interval:

Field Name	Description
Polling Interval(s)	Select the polling interval in seconds to view the real time line graph for the selected interval.

You can specify a polling interval that is greater than the QA probe polling frequency to make optimal usage of the graph.

If you launch the graph for QA probes configured on multiple nodes, you can view the following:

The X-Axis displays the unit of time, and the Y-Axis displays the selected metric for which you can view the graph.

You can view the graph of all the QA probes configured on the nodes and infer the trend of the metric for the time period. Each QA probe is identified by a unique color to distinguish the trend of all the QA probes in the graph. The color representing each QA probe appears in the legend of the graph.

If you launch the graph for selected QA probes, you can view the following:

The X-Axis displays the unit of time, and the Y-Axis displays the selected metric for which you can view the graph.

You can view the graph of the selected QA probes and infer the trend of the metric for the time period. Each QA probe is identified by a unique color to distinguish the trend of all the selected probes in the graph. The color representing each QA probe appears in the legend of the graph.

Related Topics

[Overview of Real Time Line Graph](#)

Chapter 7: Monitoring Using Reports

The NNM iSPI Performance for QA provides you with reports that enable you monitor interface health, traffic flow through a specified interface and check the health of the NNM iSPI Performance for QA.

For more information about reports, see "[Launching Source Interface Reports](#)" below and "[Launching Application Health Reports](#)" on page 130.

Launching Source Interface Reports

The NNM iSPI Performance for QA enables you to view source interfaces for the QA probes and analyze the traffic flows passing through the interface.

The NNM iSPI Performance for QA maps the interface only if the HP Network Node Manager i Software has discovered the interface and the interface information is available in the NNMi database. If the source IP is management IP, the NNM iSPI Performance for QA does not display the interface.

Using this feature, you can:


- Monitor the interface health for a specific time range.
- Monitor the traffic flow through the specified source interface for a specific time range.
- Launch the NNMi Interface form and view the interface details.

Follow any of these techniques to configure the source interface to a QA probe:

- For QA probes, specify the source IP address to the QA probe.
- For RFC 4560 QA probes or Juniper RPM QA probes, specify the source interface index when configuring the QA probes.
- You can also use the Probe Configuration form. For more information, see "[Managing QA Probes](#)" on page 313

The NNM iSPI Performance for QA maps the source IP address or the interface index configured for the QA probe to the interface in NNMi.

To launch the interface and traffic flow related reports for the source interface:

1. Click  next to the Source Interface in the QA Probes form.
2. Select **Open**.
The Interface form opens.
3. Select **Actions** and **Reporting - Report Menu** to display the reports related to the interface.

For example, the Jitter or VoIP QA probe is configured on the edge router and the edge router is multi homed with different ISPs. So the selected metrics makes more sense when the correct interface for sending the traffic is picked. So the customer configures the QA probe with an interface. In this case, the interface is stored in the DB and also dumped to HP NNM iSPI Performance for Metrics Software for reporting.

Assume that there is a threshold violation and the customer wants to see all the Top N talkers, scoped by the interface. This is achievable because the interface is stored in NPS and all reports are scoped by interface.

Customer can pick all the 'conversations' between this source and destination to find the root cause.

Launching Application Health Reports

You can check the health of the NNM iSPI Performance for QA by viewing the QA Health Report.

To launch the Application Health Report:

Select **Help** → **Help for NNM iSPIs** → **QA Application Health** from the NNMi console to check the health status of NNM iSPI Performance for QA.

The user interface displays the following tabs:

- Memory Details
- CPU Usage Details
- System Load Avg, Swap and other details
- Database Connection Details
- State Poller Health
- GNM Health

The **Memory Details** tab contains the following information:

- Name
- Status
- Used (%)
- Max (MB)
- Committed (MB)

The **CPU Usage Details** tab displays the QA CPU Utilization information only for Linux platforms:

- CPU Usage Details
- Load Average

The **System Load Avg, Swap and other details** tab contains the following information:

- Available Processors
- Free Physical Memory
- Physical Memory
- Committed Virtual Memory
- Free Swap Space
- Total Swap Space

The **Database Connection Details** tab contains the following information:

- Connections Available
- Total Connections
- Maximum Connections in Use
- Maximum Created
- Connections Destroyed
- Connections in Use

The **StatePoller** tab contains the following information:

- Collections Requested in Last 5 minutes
- Collections Completed in Last 5 minutes
- Collections in Process
- Time to Execute Skips in Last 5 minutes
- Collection Collector State Count in Last 5 minutes
- Poller result queue length 5 min(avg)

The **GNM Health** tab contains the details of the Regional Managers configured.

Chapter 8: Monitoring Using Dashboard View

The QA Performance dashboard is available in the Dashboard workspace only after you install the NNM iSPI Performance for QA. You can access the QA Performance Dashboard by clicking QA Performance in the Dashboard workspace. This dashboard displays the following tables and charts:

QA Performance Dashboard View

Dashboard Item	Display Type	Description
Probe Reachability % (avg)	Graph	The graph shows the average Probe reachability % metric value.
Probe Response Time (msecs) (avg and max)	Graph	The graph shows the average and maximum Probe Response Time metric values, in milliseconds.
Top 10 Probes by RTT (msecs) (avg)	Table	Ranks top 10 probes with the highest average Round Trip Time, in milliseconds.
Probe RTT, Jitter (msecs) (avg)	Graph	The graph shows the average Round Trip Time (RTT) and Two-Way Jitter metric values of all the probes, in milliseconds.
Interface Bandwidth Utilization % (avg)	Graph	The graph shows the average of interface bandwidth utilized by QoS classes in percentage (%).
Pre and Post Policy Rate (kbps) (avg)	Graph	The graph shows the average Pre

QA Performance Dashboard View, continued

Dashboard Item	Display Type	Description
		Policy Rate and Post Policy Rate metric values, in kbps.
Top QoS Interfaces by Bandwidth Utilization % (avg)	Table	Ranks top 10 QoS interfaces with the highest Bandwidth Utilization % metric values.
Top 10 Class Packet Drop % (avg and max)	Table	Ranks top 10 Traffic Classes with the highest and its average Class Packet Drop % metric values.
Top 10 Ping Latency Pairs by RTT (avg)	Table	Ranks top 10 Ping Latency Pairs with the highest (average) Round Trip Time in milliseconds.
Ping Latency RTT (ms) (avg)	Graph	The graph shows the average Ping Latency RTT metric values.
Ping Latency Interface Utilization % (avg)	Graph	The graph shows the average Ping Latency Interface Utilization % metric values.

Note: By default, the graph displays the line graph of the metrics. You can select the area, bar, or scatter graph for a detailed analysis.

Chapter 9: Interpreting Incidents

The NNM iSPI Performance for QA generates incidents to enable you to take appropriate action to maintain the health of your network.

For information about incidents generated by NNM iSPI Performance for QA, see the following:

- [Supported Incident Types](#)
- ["Baseline Incidents" on the next page](#)
- ["Threshold Incidents" on page 136](#)
- ["Correlated Incidents" on page 137](#)

QoS Incident Types Supported by the NNM iSPI Performance for QA

NNM iSPI Performance for QA supports the following incident types:

Metric Name	Measurement	Management Incident Name	Severity
Pre Policy Bit Rate	Kbps	PrePolicyBitRateHigh	Warning
Post Policy bit Rate	Kbps	PostPolicyBitRateHigh	Warning
Packet Drop	Percentage	PacketDropForClassHigh	Major
Exceeded Packets	Percentage	PacketsExceedingPolicedRate	Warning
Violated Packets	Percentage	PacketsViolatingPolicedRate	Major
Discarded Packets	Percentage	QueueDiscardPacketsHigh	Major
Queue Utilization	$(\text{Queue Depth}/\text{Maximum Queue Depth}) * 100$	QueueUtilizationHigh	Major
Queue Bandwidth Utilization	$(\text{PostPolicyBytesPerSecond (per class)}/\text{bandwidth}) * 100$	QueueBandwidthUtilizationHigh	Major
Dropped Shape Packets	Percentage	ShapeDroppedPacketsHigh	Warning
Delayed Shape Packets	Percentage	ShapedDelayedPacketsHigh	Warning
RED Packets Tail Drop	Percentage	REDTailDropPacketsHigh	Major
RED Packets Drop	Percentage	REDDropPacketsHigh	Major
Marked DSCP Packets	Percentage	PacketsMarkedDSCPHigh	Warning

Marked IP Precedence Packets	Percentage	PacketsMarkedIPPrecedenceHigh	Warning
Marked FRDE Packets	Percentage	PacketsMarkedFRDEHigh	Warning

Baseline Incidents

The following table lists the NNM iSPI Performance for QA baseline incidents:

Incident Name	Severity	Description
DestinationToSourceNegativeJitterAbnormal	Critical	Measured value of the negative jitter is abnormal during the baseline monitoring time.
SourceToDestinationNegativeJitterAbnormal		
DestinationToSourcePositiveJitterAbnormal	Critical	Measured value of the positive jitter is abnormal during the baseline monitoring time.
SourceToDestinationPositiveJitterAbnormal		
TwoWayJitterAbnormal	Critical	Measured value of the two-way jitter is abnormal during the baseline monitoring time.
DestinationToSourcePacketLossAbnormal	Critical	Measured value of the packet loss percentage is abnormal during the baseline monitoring time.
SourceToDestinationPacketLossAbnormal		
TwoWayPacketLossAbnormal	Critical	Measured value of the packet loss percentage is abnormal during the baseline monitoring time.
MeanOpinionScoreAbnormal	Critical	Measured value of Mean Opinion Score (MOS) is abnormal during the baseline monitoring time.
RoundTripTimeAbnormal	Critical	Measured value of

		the round trip time is abnormal during the baseline monitoring time.
--	--	--

Threshold Incidents

The following table lists the incidents raised for NNM iSPI Performance for QA threshold violations:

Incident Name	Severity	Description
DestinationToSourceNegativeJitterHigh	Critical	Measured value of the negative jitter is higher than the upper boundary of the configured threshold value.
SourceToDestinationNegativeJitterHigh		
DestinationToSourcePositiveJitterHigh	Critical	Measured value of the positive jitter is higher than the upper boundary of the configured threshold value.
SourceToDestinationPositiveJitterHigh		
TwoWayJitterHigh	Critical	Measured value of the two-way jitter is higher than the upper boundary of the configured threshold value.
DestinationToSourcePacketLossHigh	Critical	Measured value of the packet loss percentage is higher than the upper boundary of the configured threshold value.
SourceToDestinationPacketLossHigh		
TwoWayPacketLossHigh	Critical	Measured value of the packet loss percentage is higher than the upper boundary of configured threshold value.
MeanOpinionScoreLow	Critical	Measured value of Mean Opinion Score (MOS) is less than the lower boundary of the configured threshold value.
RoundTripTimeHigh	Critical	Measured value of the round trip time is higher than the upper bound of the configured threshold value.
TestDisabled	Critical	Selected QA probe is in

		Disabled state.
TestError	Warning	Selected QA probe returned an error.
TestFailed	Critical	Selected QA probe failed to run.
TestTransient	Critical	Selected QA probe is in transient state.

Correlated Incidents

The NNM iSPI Performance for QA performs root cause analysis on the failed probes and generates correlated incidents for the probes failed because of common cause. These incidents enable you to identify the cause of probe failure.

The following table lists the incidents raised and affected by NNM iSPI Performance for QA Root Cause Analysis:

Incident	Severity	Correlated Incidents
TestDestNotReachable	Critical	TestFailed
TestDestDown	Critical	TestDestNotReachable
		TestServiceDown
TestServiceNotReachable	Critical	TestFailed
TestServiceDown	Critical	TestServiceNotReachable
SiteNotReachable	Critical	TestDestDown
SiteDown	Critical	SiteNotReachable

Chapter 10: Analyzing the Root Cause of QA Probe Failure

Using root cause analysis, NNM iSPI Performance for QA performs the following tasks on the failed QA probes:

- Identifies the underlying cause when a QA probe fails to run.
- Correlates the probe failures that can be associated with the same cause.
- Generates a common incident for the QA probes failed for a common cause.
You can identify the cause of probe failure using this incident.

Causes for QA Probe Failure Between Nodes

- [When a specific source IP address fails to reach a specific destination IP address](#)

Incident Generated: TestDestNodeNotReachable

Severity: Critical

Root Cause Analysis:

- All ICMP probes from a source IP address to a destination IP address fail.
- Destination IP address cannot be reached from the source IP address.

As a result, all other QA probes configured for the destination IP address fail. The incident denotes reachability failure and correlates all the other probe failures with it.

- [When a source IP address fails to reach a specific destination IP address](#)

Incident Generated: TestDestDown

Severity: Critical

Root Cause Analysis:

- All ICMP probes from any source IP address to a specific destination IP address fail.
- Destination node is down.

As a result, all other QA probes configured for the destination IP address fail. The incident denotes that the destination node is down and correlates all the other probe failures from all source IP addresses with it.

- [When a service type fails between a source IP address and destination IP address](#)

Applicable only if more than one QA probe of the same service type runs between the selected source and destination IP addresses.

Incident Generated: TestServiceNotReachable

Severity: Critical

Root Cause Analysis:

- All probes for a service type fail between a specific source IP address and destination IP address.
- The service type is unavailable between the source and destination IP addresses.

As a result, all other QA probes of the same service type configured for the destination IP address fail. The incident denotes that the service type is unavailable and correlates all the other probe failures with it.

- [When a service type fails between any source IP address and a specific destination IP address](#)

Incident Generated: TestServiceDown

Severity: Critical

Root Cause Analysis:

- All probes for a service type fail from all source IP addresses to a specific destination IP address.
- The service type is unavailable on the destination IP address.

As a result, all other QA probes of the same service type configured for the destination IP address fail. The incident denotes that the service type on the destination node is unavailable and correlates all the other probe failures from all source IP addresses with it.

Causes for QA Probe Failure Between Sites

- [When a specific source site fails to reach a specific destination site](#)

Incidents Generated:

- SiteNotReachable

Severity: Critical

- SiteReachable

Severity: Normal

Root Cause Analysis:

- All ICMP probes from a source site to a destination site fail.
- Destination site cannot be reached from the source site.

As a result, all other QA probes configured for the destination site fail. The incident denotes reachability failure and correlates all the other probe failures with it.

- [When a source site fails to reach a specific destination site](#)

Incidents Generated:

- SiteDown

Severity: Critical

- SiteUp

Severity: Normal

Root Cause Analysis:

- All ICMP probes from any source site to a specific destination site fail.
- Destination site is down.

As a result, all other QA probes configured for the destination site fail. The incident denotes that the destination site is down and correlates all the other probe failures from all source sites with it.

- [When a service type fails between a source site and destination site](#)

Incidents Generated:

- ServiceToSiteNotReachable

Severity: Critical

- ServiceToSiteReachable

Severity: Normal

Root Cause Analysis:

- All probes for a service type fail between a specific source site and destination site.
- The service type is unavailable between the source and destination sites.

As a result, all other QA probes of the same service type configured for the destination site fail. The incident denotes that the service type is unavailable and correlates all the other probe failures with it.

- [When a service type fails between any source site and a specific destination site](#)

Incident Generated:

- ServiceToSiteDown

Severity: Critical

- ServiceToSiteUp

Severity: Normal

Root Cause Analysis:

- All probes for a service type fail from all source sites to a specific destination site.
- The service type is unavailable on the destination site.

As a result, all other QA probes of the same service type that are configured for the destination site fail. The incident denotes that the service type on the destination site is unavailable and correlates all the other probe failures from all source sites with it.

For information about the correlated incidents raised and affected by NNM iSPI Performance for QA Root Cause Analysis, see [Correlated Incidents](#).

Part II: Help for Administrators

NNM iSPI Performance for QA enables you to do the following:

- Discover the QA probes configured on NNMI-managed nodes.
- Configure QA probes.
- Configure threshold for a [Site](#)¹, QA probe, QoS element, Ping Latency pair, or QA Group.
- Organize NNM iSPI Performance for QA elements (QA probes, nodes, node groups, QoS elements, and so on) in sites based on their geographical locations.
- Organize NNM iSPI Performance for QA elements (QA probes, nodes, node groups, QoS elements, and so on) in QA groups based on any other common attribute.

You can access the [Quality Assurance Configuration Console](#) from the Configuration workspace in NNMI to configure sites, threshold, discovery filters, and global manager. However, the following configuration tasks can be performed directly in the NNMI console:

- Probe configuration
- Probe maintenance
- Threshold configuration

¹A logical organization of networking devices. In the scope of enterprise networks, a site can be a logical grouping of networking devices generally situated in similar geographic location. The location can include a floor, building or an entire branch office or several branch offices which connect to head quarters or another branch office via WAN/MAN. Each site is uniquely identified by its name. In case of the service provider networks the Virtual Routing and Forwarding (VRF) on a Provider Edge (PE) router or a Customer Edge (CE) routers can be defined as a site.

Chapter 1: About the Configuration Console

The Quality Assurance Configuration console is a separate console that contains links to user interfaces for configuring the NNM iSPI Performance for QA specific objects. Examples of objects are sites, threshold, discovery filters, and regional managers. You can do the configuration task only if you have Administrator privileges. This console also gives the configuration summary details, which displays the statistic details of the configuration.

The following configuration tasks can be performed directly in the NNMi console:

- Probe Configuration
- Probe Maintenance
- Threshold configuration for Probes

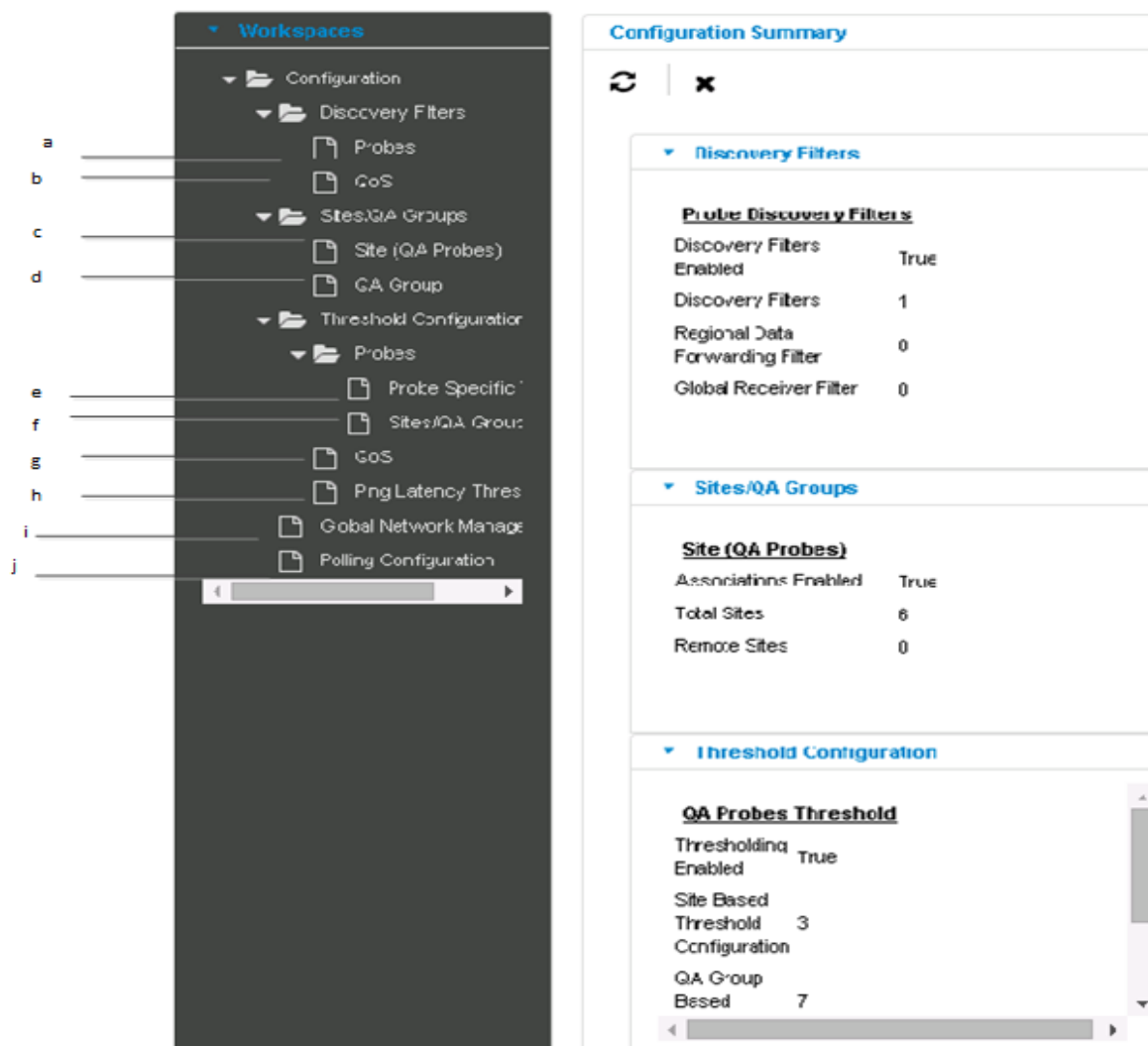
The thresholds for probes can be edited in the Probe Specific Thresholds form in the Quality Assurance Configuration console.

Launching the Quality Assurance Configuration Console

To launch the Quality Assurance Configuration console:

1. Log on to NNMi console using your user name and password.
You must have administrator privileges.
2. From the workspace navigation panel, select the **Configuration** workspace.
3. Select **Quality Assurance Configuration Console**.

The Quality Assurance Configuration console opens.



The list of configuration links appear below the **Configuration** workspace in the left pane. They are grouped into four sections namely, Discovery Filter, Sites/QA Groups, Threshold Configuration, and Global Network Management.

- a. **Probe Discovery Filter Configuration:** You can configure a discovery filter to exclude the QA probes based on some of the attributes of the QA probe.
- b. **QoS Discovery Filter Configuration:** You can configure a discovery filter to exclude the QoS elements based on some of the attributes of the QoS element.
- c. **Site (QA Probes) Configuration:** You can configure sites for a global manager or a regional manager. By grouping the networking devices into sites, you can get an overview of the network performance.
- d. **QA Group Configuration:** You can configure a QA Group based on a specific NNM iSPI Performance for QA entity type and assign all probes that belong to the same group.
- e. **Probe Specific Threshold Configuration:** You can view the list of QA probes for which you have configured the threshold, and you can edit the probe-specific threshold, if required.
- f. **QA Probes Threshold Configuration:** You can configure thresholds for all the configured sites and QA Groups.

- g. [QoS Threshold Configuration](#): You can configure thresholds for the available QoS elements in your network.
 - h. [Ping Latency Threshold Configuration](#): You can configure thresholds for the ping latency pairs in your network.
 - i. [Global Network Management Configuration](#): You can configure the regional manager specific to NNM iSPI Performance for QA using this user interface in the global manager.
 - j. [Polling Frequency Configuration](#): You can apply the QA Group based polling frequency on all the QA Groups.
4. Click the link in the left pane for configuration summary details.

The configuration summary details appear as given below:

a. **Probe Discovery Filters**

Field Name	Description
Discovery Filters Enabled	Displays the value True if discovery filters are enabled, otherwise displays the value False.
Discovery Filters	Indicates the number of discovery filters configured.
Regional Data Forwarding Filter	Indicates the number of regional data forwarding filter configured.
Global Receiver Filter	Indicates the number of global receiver filters configured.

b. **QoS Discovery Filters**

Field Name	Description
QoS Discovery Filter	Indicates the number of QoS discovery filters configured.

c. **Site (QA Probes)**

Field Name	Description
Associations Enabled	Displays the value True if the site associations are enabled, otherwise displays the value False.
Total Sites	Indicates the total number of Local Sites ¹ and Remote Sites ² configured in the NNMi management server.
Remote Sites	Indicates the number of Remote Sites ³ configured.

d. **QA Group**

¹Sites configured in the local NNMi management server are referred to as Local Sites. The local sites are owned by the Manager on which it is configured.

²Sites exported from the regional manager to the global manager are known as Remote Sites.

³Sites exported from the regional manager to the global manager are known as Remote Sites.

Field Name	Description
Probe based	Indicates the number of probes-based QA groups configured.
CBQoS based	Indicates the number of CBQoS-based QA groups configured.
PL Pair Based	Indicates the number of Ping Latency pair-based QA groups configured.

e. QA Probes Threshold

Field Name	Description
Thresholding Enabled	Displays the value True if threshold computation and association are enabled, otherwise displays the value False.
Site Based Threshold Configuration	Indicates the number of site-based thresholds configured.
QA Group Based Threshold	Indicates the number of QA group-based QA probe thresholds configured.
Probes with specific Thresholds Configured	Indicates the number of probes based threshold configured.

f. QoS Threshold

Field Name	Description
QoS Condition Based Threshold	Indicates the number of QoS thresholds configured.
QA Group Based Threshold	Indicates the number of QA group-based QoS thresholds configured.

g. Ping Latency Threshold

Field Name	Description
QA Group Based Threshold	Indicates the number of QA group-based Ping Latency thresholds configured.



h. Global Network Management

Field Name	Description
Regional Managers	Indicates the number of regional managers configured (if any) for the NNMI management server you are logged into.

i. Polling Configuration

Field Name	Description
QA Group Specific Polling	Displays the value True if the QA Group specific polling is enabled, otherwise displays the value False.

5. You can perform the following actions in the Quality Assurance Configuration console:

Icons	Description
 Close	Closes the Quality Assurance Configuration console.
 Refresh	Retrieves the last saved configuration details from the database, updates the summary details and displays the data in the Quality Assurance Configuration console.

Enabling Single Sign-On

To enable Single Sign-On between NNMi and the NNM iSPI Performance for QA (for easy access of the Quality Assurance Configuration Console):

1. Go to the following location on the NNMi management server:
On Windows:
`%nmdatadir%\shared\nnm\conf\props`
On Linux:
`/var/opt/OV/shared/nnm/conf/props`
2. Open the `nms-ui.properties` file with a text editor.
3. Make sure that the `com.hp.nms.ui.sso.isEnabled` property is set to `true`.
4. Run the following commands on the NNMi management server:
 - a. `nmssso.ovpl -reload`
 - b. `nmsqassoreload.ovpl`

Note: Do not enable the Single Sign-On feature when NNMi and the NNM iSPI Performance for QA are configured to use the Public Key Infrastructure (PKI) authentication.

For more information on the PKI authentication, see *Configuring Access with Public Key Infrastructure Authentication* section in the *NNM iSPI Performance for QA Deployment Reference*.

Chapter 2: About Discovery

NNMi spiral discovery automatically updates information after each NNMi discovery. It is a dynamic process and it continuously discovers the existence of network devices, so network changes are quickly detected. On discovering any network changes, it sends a discovery notification to NNM iSPI Performance for QA. NNM iSPI Performance for QA then looks into all the MIBs it supports to discover changes to the network elements it supports.

You can also initiate the discovery of QA probes using command line utility. For more information, see ["On-Demand Discovery" below](#). Also, you can restrict the discovery to discover only a required set of probes/QoS elements in your network by using discovery filters. For more information about discovery filters, see ["Configuring Discovery Filters" on page 156](#).

On-Demand Discovery

NNM iSPI Performance for QA discovers the QA probes configured in the network managed by NNMi during each NNMi discovery. However, if you do not want to wait till NNMi discovers, run the following command to discover the QA probes configured on the managed NNMi nodes:

```
nmsqadisco.ovpl -u <username> -p <password> [- node <nodename>][-all]
```

Parameters

- `-u <username>`: Type the NNMi administrator user name.
- `-p <password>`: Type the NNMi administrator password.
- `-node <nodename>`: Type the node name to initiate the discovery of QA probes on the selected node.
- `-all`: Type this parameter to initiate the discovery of QA probes on all the managed nodes.

Note: As a best practice, do not use the `-all` option for more than 500 nodes.

You must either use the `-node <nodename>` or the `-all` parameter to run the command.

Note: `-u <username>` `-p <password>` are optional parameters.

Chapter 3: Configuring Ping Latency Pairs

The NNM iSPI Performance for QA enables you to configure [ping latency pairs](#)¹ to monitor RTT between pairs of routers and nodes. You must define router-node pairs that you want to monitor in a configuration file. The configuration file—`PingPair.conf`—must be placed in the following location in the NNMi management server:

- Windows: `%NnmDataDir%\shared\qa\conf`
- Linux: `/var/opt/OV/shared/qa/conf`

The NNM iSPI Performance for QA installer places a sample copy of the `PingPair.conf` file in the NNMi management server. You can use the sample file as a template.

Contents of the PingPair.conf File

You can define as many router-node pairs as you like in the `PingPair.conf` file. Each line in the file contains definition of only one pair. Therefore, to define a new router-node pair, introduce a new line first.

Syntax

```
Hostname,ifName,ifIndex,ifAlias  
|DestinationName,ifName,ifAlias,ifIndex,DestinationIP|Hostname,IP
```

- The segment before the first pipe character (|) represents the details of the source router.
- The segment before the second pipe character (|) represents the details of the destination node.
- The last segment represents the details of the source proxy.

You must use the following format to define a router-node pair:

```
Source Details|Destination Details|SourceProxy Details
```

Tip: The `SourceProxy Details` segment is an optional segment. You can use this segment if you want to use a proxy router to trigger the ping request on behalf of the source router. In a Multiprotocol Label Switching (MPLS) environment, you can specify the details of the shadow router in this segment. When you omit the `SourceProxy Details` segment, the expression must contain a trailing | character, that is, `Source Details|Destination Details|`.

When specifying the entities in each segment, you must maintain the given order. Not all entities in each segment are mandatory. Each segment includes only one mandatory entity. For each optional entity you omit in a segment, you must add an additional comma before you type the next entity or the | character. For example, if you want to omit `ifIndex` and `ifAlias` in the `Source Details` segment and

¹A router-node pair used by the NNM iSPI Performance for QA to measure and monitor the connectivity between the router and the node. The router-node pair definition must be available in a configuration file provided by the NNM iSPI Performance for QA.

ifName, ifAlias, and ifIndex in the Destination Details segment, then the definition must look like this:

```
Hostname,ifName,,|DestinationName,,,,DestinationIP|
```

Segments of a Pair Definition

The following sections list the segments of a router-node pair definition:

Source Details

The Source Details segment includes the following entities:

Entity	Description
Host Name	<i>This is a mandatory entity.</i> The fully qualified domain name of the source router. The router must be an NNMI-managed node. You must specify the same FQDN that appears in the NNMI console.
IfName	The name of the interface that triggers the ping request.
IfIndex	A number for identifying the above interface. This value must be same as the ifIndex reported from the MIB.
IfAlias	Use this Interface MIB variable as an additional filter to identify the interfaces to include when creating the subnet connections. This attribute is useful if you have an alias naming convention that is used to identify a set of interfaces. For example, Connection to remote store in Hawaii. Maximum 255 characters. The following wildcard characters are allowed: Asterisk (*) represents any string Question mark (?) represents a single character

Destination Details

The Destination Details segment includes the following entities:

Details	Description
Host Name	The name that is assigned to any device within a network, for identification
IfName	The name of the interface that receives the ping request.
IfIndex	A unique number for identifying an interface. Example: 12345
IfAlias	Use this Interface MIB variable as an additional filter to identify the interfaces to include when creating the subnet connections. This attribute is useful if you have an alias naming convention that is used to identify a set of interfaces. For example, Connection to remote store in Hawaii. Maximum 255 characters. The following wild card characters are allowed:

Details	Description
	Asterisk (*) represents any string Question mark (?) represents a single character
Dest_ IPAddress	<i>This is a mandatory entity.</i> The IP address of the destination. You must specify the destination IP address for the ping pair destination information.

SourceProxy Details

The SourceProxy segment includes the following entities:

Details	Description
Host Name	The fully qualified domain name of the router that triggers the ping request on behalf of the source router. If you want to use a source proxy, make sure that the proxy router is managed by NNMi and the Write community string is configured on the router.
Proxy_ IP	The IP address of the proxy router.

Configuring Ping Pairs

To configure the ping latency pairs in the `PingPair.conf` file, you must have an administrator's or root access to the NNMi management server where you installed the NNM iSPI Performance for QA.

To configure router-node pairs:

1. Identify the routers in your environment from which you want to trigger ping requests. If you do not have adequate rights on a router, you can use a proxy router for the purpose of triggering the ping request. The source routers (and proxy routers) must be managed by NNMi and the Write community string must be enabled on source routers.
2. Identify the nodes to which you want to send the ping requests.
3. Log on to the NNMi management server as administrator or root.
4. Go to the following directory:
Windows: %NnmDataDir%\shared\qa\conf
Linux: /var/opt/OV/shared/qa/conf
5. Open the `PingPair.conf` file with a text editor.
6. Add router-node pair definitions. Each line in the file can contain only one definition. Introduce a new line before adding a new pair definition. While typing the definitions, follow the guidelines provided in "[Contents of the PingPair.conf File](#)" on page 151.
7. Save the file.

During the subsequent polling cycle of the NNM iSPI Performance for QA, all routers defined in the `PingPair.conf` file start triggering ping requests. NNM iSPI Performance for QA continue to trigger ping requests from the source node at the frequency of 300 sec by default. You can define

the custom polling interval in the `PingPairPoll.conf` file. For more information about attributes for ping request, see ["Default Attributes of Each Ping Request" below](#).

If the `PingPair.conf` file is deleted from the NNMi management server, you can do one of the following:

- Add a backed-up copy of the old the `PingPair.conf` file in the appropriate directory (see [step 4](#)).
- Recreate the `PingPair.conf` file:
 - a. Add an empty text file in the directory where the file was present (see [step 4](#)).
 - b. Save the text file as `PingPair.conf`.
 - c. Add router-node pair definitions with the help of the information in ["Contents of the PingPair.conf File" on page 151](#).

In both cases, you must run the following command for the change to take effect:

- **Windows:** `%nminstalldir%\bin\nmsgapingpairconfig.ovpl -u <admin_user> -p <admin_password> -resyncConfig`
- **Linux:** `/opt/OV/bin/nmsgapingpairconfig.ovpl -u <admin_user> -p <admin_password> -resyncConfig`

In this instance, `<admin_user>` is an NNMi administrator and `<admin_password>` is the password of the NNMi administrator.

Configuring Default Ping Attributes

The size and frequency of ping requests are defined in the `PingPairPoll.conf` file by different properties. The NNM iSPI Performance for QA installer places the file on the NNMi management server. The table below lists the default attribute values:

Default Attributes of Each Ping Request

Attribute	Default Value
Packet count of each ping request	5
Size of each packet	100 bytes
Packet time-out	2000 milliseconds
Polling interval (the interval between two consecutive ping requests)	300 seconds

To change the default attribute values, you must edit the `PingPairPoll.conf` file.

To configure the default ping attributes:

1. Log on to the NNMi management server as administrator or root.
2. Go to the following directory:
 - Windows: `%NnmDataDir%\shared\qa\conf`
 - Linux: `/var/opt/OV/shared/qa/conf`
3. Open the `PingPairPoll.conf` file with a text editor. Uncomment the lines having the polling attributes.
4. Specify values of your choice for the following properties:

Property	Description
PacketCount	Packet count of each ping request
PacketSize	Size of each packet (in bytes)
PollingInterval	Polling interval (the interval between two consecutive ping requests, in seconds)
PacketTimeOut	Packet time-out (in milliseconds)

5. Save the file.
6. For the configuration to take effect, restart the NNM iSPI Performance for QA processes:
 - a. **ovstop -c qajboss**
 - b. **ovstart -c qajboss**

Chapter 4: Configuring Discovery Filters

You can have numerous probes configured in your entire network, but not all the QA probes are always useful to analyze, monitor, or measure the network performance. You can restrict the discovery to discover and monitor only a required set of probes in your network by using probe discovery filters.

Similarly, you may have numerous QoS elements (policies and classes) configured in your entire network. However, you may not need all of these QoS elements to analyze, monitor, or measure the performances of the business-critical network elements. You can restrict NNMi to discover, and NNM iSPI Performance for QA to monitor only a required set of QoS elements in your network using QoS discovery filters.

As an NNM iSPI Performance for QA administrator, you may want to perform the following tasks:

- [Configure File-Based Node Discovery](#)
- [Configure Probe Discovery Filters](#)
- [Configure QoS Discovery Filters](#)

Configuring File-Based Node Discovery

The file based node discovery configuration enables you to configure the NNM iSPI Performance for QA to exclude a set of nodes from being discovered in the network. This configuration setting can also be used to discover and monitor the QA data only for certain set of nodes.

File-Based Node Exclusion

To exclude a set of nodes from being discovered in the network, perform the following steps:

1. Create a file `discovery.exclude` at the following location:
Linux: `/var/opt/OV/shared/qa/conf`
Windows: `%NnmDataDir%\shared\qa\conf`
2. Update the file with the list of IP addresses of the nodes (one in each line) that you do not want to discover. You can also define an IP address range or use wild card character * (asterisk).
3. Save and close the file.
4. Synchronize the configuration by running the following command:
`nmsqadisco.ovpl -resyncConfig`

The nodes listed in the `discovery.exclude` file are ignored and the remaining nodes are discovered.

Note: If an already discovered node is listed in the exclusion filter, the discovery for that node stops but the polling continues for the existing QA data.

If a new node is seeded to the network and is listed in the exclusion filter, it will not be discovered by the NNM iSPI Performance for QA.

File-Based Node Inclusion

To discover a set of nodes in the network, perform the following steps:

1. Create a file `discovery.include` at the following location:
Linux: `/var/opt/OV/shared/qa/conf`
Windows: `%NnmDataDir%\shared\qa\conf`
2. Update the file with the list of IP addresses of the nodes (one in each line) that you want to discover. You can also define an IP address range or use wild card character * (asterisk).
3. Save and close the file.
4. Synchronize the configuration by running the following command:
`nmsqadisco.ovpl -resyncConfig`

Only the nodes listed in the `discovery.include` file are discovered and the remaining nodes are ignored.

Note: If an already discovered node is not listed in the in the `discovery.include` file, the discovery for that node stops but the polling continues for the existing QA data.

If a new node is seeded to the network and is listed in the inclusion filter, it will be discovered by the NNM iSPI Performance for QA.

Note: If both `discovery.exclude` and `discovery.include` files are available, only the nodes listed in the `discovery.include` file are discovered in the network.

To define an IP address range or to use wild card character, follow the rules given below:

- You can use "-" (the character hyphen) while defining an IP address range. For example, 192.168.4-9.137
- Specify the range in ascending order, that is, the range must be from a lower value to a higher value.
- Use the wild card character "*" to specify IP range between 0 to 255.
- Addresses like 0.0.0.0 and 127.0.0.1 are considered as invalid.

Configuring Probe Discovery Filters

Discovery filter allows you to exclude the QA probes (such as the interface health reporting QA probes) that produce a lot of output, and is not necessary for monitoring the network performance. It enables you to filter the discovery process, and exclude the QA probes based on the following attributes of the QA probe:

- Owners associated with the QA probes
- IP addresses of the source or destination device for which the QA probe is configured
- Service types of the QA probe


If you filter the QA probes based on different attributes, the QA probes are excluded or filtered only if it fulfills all the criteria specified in this user interface. For example, if you specify the filters based on Owners, and Service, the discovery filter ensures that it meets the criteria and excludes only those QA probes.

After you apply the filters, the filtered QA probes are removed from the database. The poller stops polling these QA probes, which get excluded from the [QA Probes](#) view.

You cannot apply discovery filters in a Global Network Management environment. The discovery filters applied in the regional manager do not get reflected in the global manager. Similarly, discovery filters applied on the global manager applies only on the data polled by the global manager, and not on the data forwarded by the regional managers.

Adding Probe Discovery Filters

To add a new discovery filter, follow the steps given below:


1. [Launch the Discovery Filter Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Discovery Filters > Probes**. The Discovery Filter Configuration form opens.
2. Select **Enable Discovery Filters** to activate the discovery filters.
3. Click  **New** in the **Configured Filters** panel in the Discovery Filter Configuration form. The Add Discovery Filter form opens.
4. Enter the following:
 - a. **Name**
A name to identify the discovery filter. The name must not contain ' (single quotation marks).
 - b. **Type**
Select the type of discovery filter. The valid options are as listed below:


- **Discovery:** Select this option to **exclude** the QA probes discovered in the network.
- **Global Receiver:** Select this option to **exclude** the QA probes received by the global manager. This option appears only for global manager.
- **Regional Data Forwarding:** Select this option to **exclude** the QA probes forwarded to the global manager. This filter is configured in the regional manager.


c. Owner Names

Type the QA probe owner name or a pattern suggesting the owner name to be filtered in the Owner Names box.


You can specify a range of QA probe owner names using the wildcard character ? (to replace one character) and * (to replace multiple characters). This field is case-sensitive.


Click  **Add**. The new QA probe owner name is added to the list in the Owner Names box.


You can select a QA probe owner name, and click  **Delete** to remove it from the Owner Names box.

You can click  **Delete All** to select all the QA probe owner names listed in the Owner Names box and remove them.

d. Source IP Addresses

Type the Source IP address or IP address range to be filtered and click  **Add**. You can add IPv4 and IPv6 addresses. If the Source IP Address is not configured, you can enter the Management IP Address.

Select a Source IP address or IP address range and click  **Delete** to remove it from the Source IP Addresses box.

You can click  **Delete All** to remove all the IP addresses listed in the Source IP Addresses box.

Follow the rules given below, when defining an IP address range:

- For IPv4 addresses, you can use "-" (the character hyphen) when defining a range of IPv4 addresses.
- Specify the range in the ascending order. The range must be from a lower value to a higher value.
- For IPv4 addresses, use the wild card character "*" to specify IP addresses between 0 to 255.
- For both IPv4 and IPv6, specify an IP address range using "-" (hyphen).
- For both IPv4 and IPv6, specify the IP address range in the ascending order. For example, 16.*.*, 17.1-100.*.*.
- For IPv4, addresses such as 0.0.0.0 and 127.0.0.1 are considered invalid.
- For IPv6 addresses, use the [standard IPv6 shorthand notation](#).

e. Destination IP Addresses

Type the Destination IP address or IP address range to be filtered and click

Add

Add. You can add IPv4 and IPv6 addresses.

Select an IP address or IP address range and click **Delete** to remove it from the Destination IP Addresses box.

You can click **Delete All** to remove all the addresses listed in the Destination IP Addresses box.

Follow the rules given below, when defining an IP address range:

- For IPv4 addresses, you can use "-" (the character hyphen) when defining a range of IPv4 addresses.
- Specify the range in the ascending order. The range must be from a lower value to a higher value.
- For IPv4 addresses, use the wild card character "*" to specify IP addresses between 0 to 255.
- For both IPv4 and IPv6, specify an IP address range using "-" (hyphen).
- For both IPv4 and IPv6, specify the IP address range in the ascending order. For example, 16.*.* , 17.1-100.*.*.
- For IPv4, addresses such as 0.0.0.0 and 127.0.0.1 are considered invalid.
- For IPv6 addresses, use the [standard IPv6 shorthand notation](#).

f. **Service**

Select one or more of the following services to filter and click **Add**.

- UDP Echo
- ICMP Echo
- UDP
- TCP Connect
- VoIP
- ICMP Jitter
- HTTP
- HTTPS
- DNS
- Oracle
- DHCP




The service is added to the list in the Service box.

Select the service, and click **Delete** to remove it from the Service box.


You can click **Delete All** to remove all the services listed in the box.


The QA probes are excluded or filtered only if it fulfills all the criteria specified in this user interface. For example, if you specify the filters based on Owners, and Service, the discovery filter ensures that it meets both the criteria and excludes only those QA probes.

5. You can perform the following tasks:

Icon	Description
 Close	Closes the Discovery Filter Configuration form without saving the filter information you have entered.
 Save	Saves the new discovery filter information.
 Save and Close	Saves the discovery filter information and closes the Discovery Filter Configuration form.

You can perform the following tasks in the Discovery Filter Configuration form.:

Icon	Description
Enable Discovery Filters (in the Global Settings Panel)	Selecting this check box enables the filters to be applied for subsequent discoveries. If this check box is not selected, you will not be able to click on  Apply Filter Now .


Clicking the  **Apply Filter Now** applies the discovery filters and deletes the filtered local QA Probes from the database. This functionality is applicable only for [Local QA Probes](#)¹ and Discovery filter type.

The Registration panel provides the following detail about the selected discovery filter:

Attribute	Description
Last Modified Date	Date when the selected discovery filter was last modified.

Editing Probe Discovery Filters

To edit a discovery filter:

1. [Launch the Discovery Filter Configuration form](#).
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Discovery Filters > Probes**. The Discovery Filter Configuration form opens.
2. Select a filter in the **Configured Filters** tab, and click  **Edit**.
The Edit Discovery Filter form opens.
3. Select **Enable Discovery Filters** option to activate the discovery filters.
4. Update the following values as required:

¹Local QA probes are QA probes owned by the local sites.

a. **Name**

A unique name to identify the discovery filter. The name must not contain ' (single quotation marks).

b. **Type**

Select the type of discovery filter. The valid options are listed below:


- **Discovery:** Select this option to **exclude** the QA probes discovered in the network.
- **Regional Data Forwarding:** Select this option to **exclude** the QA probes forwarded to the global manager.
- **Global Receiver:** Select this option to **exclude** the QA probes received by the global manager. This option appears only for global manager.


The following fields appear only if you select the type of discovery filter.


c. **Owner Names**

Type the QA probe owner name or a pattern suggesting the owner name to be filtered in the Owner Names box .


You can specify a range of QA probe owner names using the wildcard character ? (to replace one character) and * (to replace multiple characters). This field is case-sensitive.


Click  **Add**. The new QA probe owner name is added to the list in the Owner Names box.


You can select a QA probe owner name, and click  to remove it from the Owner Names box.

You can click  **Delete All** to select all the QA probe owner names listed in the Owner Names box and remove them.

d. **Source IP Addresses**

Type the Source IP address or IP address range to filter and click  **Add**. You can add IPv4 and IPv6 addresses. If the Source IP Address is not configured, you can enter the Management IP Address.

Select a Source IP address or IP address range and click  **Delete** to remove it from the Source IP Addresses box.


You can click  **Delete All** to remove all the addresses listed in the Source IP Addresses box.

Follow the rules given below, when defining a Source IP address range:

- For IPv4 addresses, you can use "-" (the character hyphen) when defining a range of IPv4 addresses.
- Specify the range in the ascending order. The range must be from a lower value to a higher value.
- For IPv4 addresses, use the wild card character "*" to specify IP addresses between 0 to 255.

- For both IPv4 and IPv6, specify an IP address range using "-" (hyphen).
- For both IPv4 and IPv6, specify the IP address range in the ascending order. For example, 16.*.*, 17.1-100.*.*.
- For IPv4, addresses such as 0.0.0.0 and 127.0.0.1 are considered invalid.
- For IPv6 addresses, use the [standard IPv6 shorthand notation](#).

e. **Destination IP Addresses**

Type the Destination IP address or IP address range to filter and click  **Add**. You can add IPv4 and IPv6 addresses. Select a Destination IP address or IP address range and click

 **Delete**

to remove it from the Destination IP Addresses box.

 **Delete All**

You can click **Delete All** to remove all the addresses listed in the Destination IP Addresses box.

Follow the rules given below, when defining an IP address range:

- For IPv4 addresses, you can use "-" (the character hyphen) when defining a range of IPv4 addresses.
- Specify the range in the ascending order. The range must be from a lower value to a higher value.
- For IPv4 addresses, use the wild card character "*" to specify IP addresses between 0 to 255.
- For both IPv4 and IPv6, specify an IP address range using "-" (hyphen).
- For both IPv4 and IPv6, specify the IP address range in the ascending order. For example, 16.*.*, 17.1-100.*.*.
- For IPv4, addresses such as 0.0.0.0 and 127.0.0.1 are considered invalid.
- For IPv6 addresses, use the [standard IPv6 shorthand notation](#).

f. **Service**

Select one or more of the following services to filter from the drop-down list, and click

 **Add**

- UDP Echo
- ICMP Echo
- UDP
- TCP Connect
- VoIP
- ICMP Jitter
- HTTP
- HTTPS
- DNS
- Oracle
- DHCP




The service is added to the list in the Service box.
Select the service, and click

 **Delete** to remove it from the Service box.

You can click  **Delete All** to remove all the services listed in the box.




The QA probes are excluded or filtered only if it fulfills all the criteria specified in this user interface. For example, if you specify the filters based on Owners, and Service, the discovery filter ensures that it meets both the criteria and excludes only those QA probes.

5. You can perform the following tasks:

Icon	Description
 Close	Closes the Discovery Filter Configuration form without saving the filter information you have entered.
 Save	Saves the new discovery filter information.
 Save and Close	Saves the discovery filter information and closes the Discovery Filter Configuration form.

Deleting Probe Discovery Filters

To delete an existing discovery filter:


1. [Launch the Discovery Filter Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Discovery Filters** > **Probes**. The Discovery Filter Configuration form opens.
2. Select a filter in the **Configured Filters** panel, and click  **Delete**.
or
Click  **Delete All** to delete all the discovery filters.
3. Click  **Refresh** in the **Configured Filters** panel to view the changes.

After you delete a discovery filter, the filtered probes are discovered in the next discovery cycle.

Exporting Probe Discovery Filters

To export the existing discovery filter configurations to an XML file:

1. [Launch the Discovery Filter Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Discovery Filters** > **Probes**. The Discovery Filter Configuration form opens.

2. Click  **Export**.
3. Enter the file name where you want to export the existing discovery filter configuration in the user prompt dialog.

You must enter the file name with full path information. For example, C:\temp\disco_filter_conf.xml

If you enter the XML file name without entering the absolute path, by default the file is saved in the following directory:

Linux: `$NnmDataDir/shared/qa/conf`

Windows: `%NnmDataDir%\shared\qa\conf`

4. Click **OK** in the user prompt dialog.

You can also export the existing discovery filter using the following command line utility:

Linux: `$NnmInstallDir/bin/nmsqadiscofilter.ovpl -u <username> -p <password> -export <filename>`

Windows: `%NnmInstallDir%\bin\nmsqadiscofilter.ovpl -u <username> -p <password> -export <filename>`

If the discovery filter export fails, check the following log files:

Linux: `$NnmDataDir/log/qa/qa.log`


Windows: `%NnmDataDir%\log\qa\qa.log`

Note: `-u <username> -p <password>` are optional parameters.

Importing Probe Discovery Filters

To import discovery filter configurations from an XML file:

1. [Launch the Discovery Filter Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Discovery Filters** > **Probes**. The Discovery Filter Configuration form opens.

2. Click  **Import**.
3. In the user prompt dialog box, enter the file name from where you want to import the discovery filter configuration information.

You must enter the file name with full path information. For example, C:\temp\disco_filter_conf.xml

4. Click **OK**.

If a discovery filter is already defined and displayed in the Discovery Filter Configuration form, the import utility does not import the configuration information for this discovery filter from the XML file.

You can also import discovery filter using the following command line utility:

Linux: `$NnmInstallDir/bin/nmsqadiscofilter.ovpl -u <username> -p <password> -import <filename>`

Windows: %NnmInstallDir%\bin\nmsqadiscoverfilter.ovpl -u <username> -p <password> -import <filename>

If the discovery filter import fails, check the following log files:

Linux: \$NnmDataDir/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Note: When you import a discovery filter from the previous version of NNM iSPI Performance for QA, the discovery filter name is automatically generated in this version of NNM iSPI Performance for QA.

Note: -u <username> -p <password> are optional parameters.

Applying On-Demand Probe Discovery Filter

You can also apply the probe discovery filter using the `nmsqadiscoverfilter.ovpl` command:

Usage:

```
nmsqadiscoverfilter.ovpl -c [Probe] apply
```

Parameters

- -u <username>: Type the NNMi administrator user name.
- -p <password>: Type the NNMi administrator password.
- -c [Probe]: Type this parameter to apply the discovery filter for QA probes.
- -apply: Type this parameter to initiate the discovery filtering on local probes.

Note: -u <username> -p <password> are optional parameters.

Configuring QoS Discovery Filters

This feature allows you to exclude the QoS elements that may not be required for monitoring the network performance.

The Discovery Filter Configuration enables you to filter the discovery process, and exclude the QoS elements based on the following attributes:

- QoS Policy Name
- QoS Class Name
- IP Range
- Node Group
- QoS Action Name

If you filter the QoS elements based on different attributes, the QoS elements are excluded or filtered only if it fulfills **all** the criteria specified in the discovery filter. For example, if you create a QoS discovery filter called Filter A based on Class Name, and Node Group, the discovery filter ensures that it meets both the criteria and excludes only those QoS elements.

You can also configure discovery filters for the following policy types:


- A parent policy, that is, a policy that contains references to other policies, known as child policies. You can define discovery filters only on the parent policies. However, NNM iSPI Performance for QA applies the parent policy filters on the classes configured for the child policies too.
- An independent policy, that is, a policy that does not refer to any other policies.

After creating the filters, NNM iSPI Performance for QA stops polling the filtered QoS interfaces, policies, classes, and actions in the next polling cycle. As a result, the excluded QoS elements get excluded from the related views.

You cannot apply QoS discovery filters in a Global Network Management environment. The QoS discovery filters applied in the regional manager do not get reflected in the global manager. Similarly, the QoS discovery filters applied on the global manager applies only on the data polled by the global manager, and not on the data forwarded by the regional managers.

Adding QoS Discovery Filters

To add a new QoS discovery filter:

1. [Launch the QoS Discovery Filter Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Discovery Filters** > **QoS**. The QoS Discovery Filter Configuration form opens.
2. Click  **New** in the **Configured Filters** panel in the QoS Discovery Filter Configuration form.

The Add QoS Discovery Filter form opens.




3. Specify the following criteria. The QoS elements are excluded or filtered only if they fulfill all the criteria specified in this form. For example, if you specify the filters based on Policy Name and Node Groups, the discovery filter ensures that it meets both the criteria and excludes only those QoS elements.

a. **QoS Filter Name**

A unique name to identify the QoS discovery filter. The name must not contain ' (single quotation marks) or special characters. This field supports only alphanumeric characters.

b. **Policy Name**




Name of the Policy map for the QoS element that you want to exclude from the next discovery. After specifying a policy name, click any of the following buttons:

- Click  **Add**. The policy name is added to the list of policy names.
- You can select a policy name, and click  to remove it from the list of policy names.
- You can click  **Delete All** to remove all the policy names from the list.

c. **Class**

Name of the class configured for the QoS element that you want to exclude from the next discovery. For example, if you do not want to discover the classmap called ClassDefault, you can use this criteria to stop polling all QoS elements that have this classmap configured.




After specifying a class name, click any of the following buttons:

- Click  **Add** to add the class name to the list of class names.
- You can select a class name, and click  to remove it from the list of class names.
- You can click  **Delete All** to remove all the class names from the list.

d. **Action**

Name of the action configured on the QoS elements that you want to exclude from the next discovery.

After specifying a action, click any of the following buttons:




- Click  **Add** to add the action to the list of actions.
- You can select a action, and click  to remove it from the list of actions.
- You can click  **Delete All** to remove all the actions from the list.

e. **IP Range**

The IP address range for the QoS elements that you want to exclude from the next discovery. Follow the rules as discussed below, while defining a IP address range:

- For IPv4 addresses you can use "-" (the character hyphen) while defining a range of IPv4 addresses.
- Specify the range in ascending order. The range must be from a lower value to a higher value.
- For IPv4 addresses use the wild card character "*" to specify IP addresses between 0 to 255.
- For both IPv4 and IPv6, specify an IP address range using "-" (hyphen).
- For both IPv4 and IPv6, specify the IP address range in ascending order. For example, 16.*.*, 17.1-100.*.*.
- For IPv4, addresses like 0.0.0.0 and 127.0.0.1 are considered as invalid.
- For IPv6 addresses use the [standard IPv6 shorthand notation](#).

After specifying an IP range, click any of the following buttons:




- Click  **Add** to add the IP range to the list of IP ranges.
- You can select an IP range, and click  to remove it from the list of IP ranges.
- You can click  **Delete All** to remove all the IP ranges from the list.

f. Node Group

The node group name for the QoS elements that you want to exclude from the next discovery




You must create a QoS node group in NNMi before using the node group for creating a discovery filter.


After specifying a node group, click any of the following buttons:

- Click  **Add** to add the node group to the list of node groups.
- You can select a node group, and click  to remove it from the list of node groups.
- You can click  **Delete All** to remove all the node groups from the list.

NNM iSPI Performance for QA enables you to use wildcard characters to define a discovery filter criteria.

4. Click any of the following buttons to complete the task:

Icons	Description
 Close	Closes the QoS Discovery Filter Configuration form without saving the filter information you have entered.
 Save	Saves the new QoS discovery filter information
 Save and Close	Saves the QoS discovery filter information and closes the QoS Discovery Filter Configuration form


Click  **Apply Filter Now** in the QoS Discovery Filter Configuration form to apply the discovery filter immediately on the discovered QoS elements. The QoS elements affected by the modified discovery filters are not discovered in the next discovery cycle.

By default NNM iSPI Performance for QA discovers the changes in the discovery filters during each discovery cycle, and applies them on the respective QoS element. Clicking this button applies the following changes to the discovery filter:

- If you create a new QoS discovery filter
- If you edit an existing QoS discovery filter to associate it to a new policy, class, action, IP address range, or node group
- If you delete existing QoS discovery filters

Editing QoS Discovery Filters

To edit a QoS discovery filter:




1. [Launch the QoS Discovery Filter Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Discovery Filters** > **QoS**. The QoS Discovery Filter Configuration form opens.
2. Select a filter in the **Configured Filters** tab in the QoS Discovery Filter Configuration Form, and click  **Edit**.

The Edit QoS Discovery Filter form opens.

3. Update the following values as required:
 - a. **QoS Filter Name**
 - b. **Policy Name**
 - c. **Class**
 - d. **Action**
 - e. **IP Range**
 - f. **Node Group**

For details about these fields, see [Adding QoS Discovery Filters](#).




4. Use any one of the following options to complete the task:

Icons	Description
 Close	Closes the QoS Discovery Filter Configuration form without saving the filter information you have entered
 Save	Saves the new QoS discovery filter information
 Save and	Saves the QoS discovery filter information and closes the Discovery Filter Configuration form

Icons	Description
Close	

Deleting QoS Discovery Filters

To delete an existing QoS discovery filter:


1. [Launch the QoS Discovery Filter Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Discovery Filters** > **QoS**. The QoS Discovery Filter Configuration form opens.
2. Select a filter in the **Configured Filters** panel in the Discovery Filter Configuration Form, and click  **Delete**.
or
Click  **Delete All** to delete all the discovery filters.
3. Click  **Refresh** in the **Configured Filters** panel to view the changes.

After you delete a QoS discovery filter, the filtered QoS elements are discovered in the next discovery cycle.

To refresh the QoS Policies Inventory view based on the deleted filter immediately, run the discovery process after you delete the discovery filter.

Exporting QoS Discovery Filters

To export the existing QoS discovery filter configurations to an XML file:

1. [Launch the QoS Discovery Filter Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Discovery Filters** > **QoS**. The QoS Discovery Filter Configuration form opens.
2. Click  **Export**.
3. In the user prompt dialog, enter the file name where you want to export the existing QoS discovery filter configuration.

You must enter the file name with full path information; for example, C:\temp\CBQoS_disco_filter_conf.xml

If you enter the XML file name without entering the absolute path, by default the file gets saved in the following directory:

Linux: \$NmDataDir/shared/qa/conf

Windows: %NnmDataDir%\shared\qa\conf

4. Click **OK** in the user prompt dialog.

You can also export the existing QoS discovery filter using the following command line utility:

Linux: \$NnmInstallDir/bin/nmsqadiscofilter.ovpl -u <username> -p <password> -c CBQoS -export <filename>

Windows: %NnmInstallDir%\bin\nmsqadiscofilter.ovpl -u <username> -p <password> -c CBQoS -export <filename>

If the QoS discovery filter export fails, check the following log files:

Linux: \$NnmDataDir/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Note: -u <username> -p <password> are optional parameters.

Importing QoS Discovery Filters

To import QoS discovery filter configurations from an XML file:

1. [Launch the QoS Discovery Filter Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Discovery Filters** > **QoS**. The QoS Discovery Filter Configuration form opens.

2. Click  **Import**.

3. In the user prompt dialog, enter the file name from where you want to import the QoS discovery filter configuration information.

You must enter the file name with full path information; for example, C:\temp\CBQoS_disco_filter_conf.xml

4. Click **OK** in the user prompt dialog.

If a QoS discovery filter is already defined and displayed in the QoS Discovery Filter Configuration form, the import utility does not import the configuration information for this QoS discovery filter from the XML file.

You can also import discovery filter using the following command line utility:

Linux: \$NnmInstallDir/bin/nmsqadiscofilter.ovpl -u <username> -p <password> -c CBQoS -import <filename>

Windows: %NnmInstallDir%\bin\nmsqadiscofilter.ovpl -u <username> -p <password> -c CBQoS -import <filename>

If the QoS discovery filter import fails, check the following log files:

Linux: . \$NnmDataDir/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Note: While you import a QoS discovery filter from the previous version of NNM iSPI Performance for QA, the discovery filter name is automatically generated in this version of NNM iSPI Performance for QA.

Note: `-u <username>` `-p <password>` are optional parameters.

Applying On-Demand QoS Discovery Filter

You can also apply the QoS discovery filter using the `nmsqadiscoverfilter.ovpl` command:

Usage:

```
nmsqadiscoverfilter.ovpl -c [CBQoS] apply
```

Parameters

- `-u <username>`: Type the NNMi administrator user name.
- `-p <password>`: Type the NNMi administrator password.
- `-c [CBQoS]`: Type this parameter to apply the discovery filter for QoS elements in your network.
- `-apply`: Type this parameter to initiate the discovery filtering on QoS elements.

Note: `-u <username>` `-p <password>` are optional parameters.

Troubleshooting Discovery Filter Configuration Error Messages

The error log files are available in the following directory:

Linux: `./var/opt/OV/log/qa/qa.log`

Windows: `%Nnmdatadir%\log\qa\qa.log`

[QA probe filtering is not enabled. Please enable it.](#)

Occurs if you have not enabled the Enable Discovery Filters option in the Discovery Filter Configuration form.

Reason and Resolution

Select the Enable Discovery Filters option in the Discovery Filter Configuration form.

[Failed to import the discovery filter configuration. Please check the log files.](#)

Occurs if the import file does not exist in the path you entered.

Reason and Resolution

NNM iSPI Performance for QA imports the discovery filter configuration from an XML file. If the file path is not correct, NNM iSPI Performance for QA fails to import the configuration information.

Check any of the following log files:

Linux: `./var/opt/OV/log/qa/qa.log`

Windows: `%Nnmdatadir%\log\qa\qa.log`

[Failed to export the discovery filter configuration. Please check the log files.](#)

Occurs if the export file path that you entered is incorrect.

Reason and Resolution

NNM iSPI Performance for QA exports the discovery filter configuration to an XML file. If the file path is not correct, NNM iSPI Performance for QA fails to export the configuration information.

Check any of the following log files:

Linux: `./var/opt/OV/log/qa/qa.log`

Windows: `%nnmdatadir%\log\qa\qa.log`

[Invalid QA probe owner name pattern.](#)

Occurs if the Exclude Probe Owner Name Patterns field in the Discovery Filter Configuration form contains any illegal character.

Reason and Resolution

Avoid using '(Single quotation) as a QA probe owner name. NNM iSPI Performance for QA does not accept this character in a QA probe owner name.

Invalid Filter Name

Occurs when you try to save the discovery filter configuration details with an invalid filter name

Reason and Resolution

Avoid using '(Single quotation) in the filter name. NNM iSPI Performance for QA does not accept this character in a filter name.

Service Already Chosen

Occurs when you selected a service from the Service drop down list in the Discovery Filter Configuration form

Reason and Resolution

Do not select the same service again and add to the list.

Chapter 5: Configuring Sites

NNM iSPI Performance for QA enables you to monitor the network performance of different [network elements](#)¹. Logically grouping the networking devices into [sites](#)² enables to monitor a similar set of QA probes.

Example

An enterprise network with branch offices is connected to the head office via WAN links. You can measure the network performances across all the offices and compare the network performance of the head office and the branch offices. This is useful to get an overview of health or performance of the network.

You can configure QA probes between individual nodes or node groups and assign them to the sites. Also, you can configure the threshold for a site using the Threshold Configuration form. The threshold configured for a site is applied to all the QA probes of that site. This procedure takes very less time compared to configuring the threshold for each probe. You can view the measured value of the metrics for a site, which enables you to analyze the site and inter-site performance as well.

In a Global Network Management (GNM) environment, you can configure sites on a global manager or a regional manager. Based on this configuration, sites can be categorized as follows:

- **Local Sites:** Sites configured in the local NNMi management server are referred to as Local Sites. The local sites are owned by the manager on which it is configured.
- **Remote Sites:** The sites exported from the regional manager to the global manager are known as Remote Sites.

Whenever you create, edit, or delete a site in the regional manager, the changes are propagated to the global manager. You can export local sites, but you cannot export or delete remote sites. The advantage of exporting sites is that you need not configure the sites again.

Note: The sites configured and exported in the previous version of NNM iSPI Performance for QA can be imported and used in this version as well. For more information about importing sites, see ["Importing Sites " on page 191](#).

QA Probes Association

QA probes can be associated with either a local site or a remote site. Probes can be categorized as follows:

- **Local QA Probes:** Local QA probes are QA probes owned by the local manager.
- **Remote QA Probes:** Remote QA probes are primarily discovered and polled at the regional manager.

¹Some examples of network elements are routers and switches.

²A logical organization of networking devices. In the scope of enterprise networks, a site can be a logical grouping of networking devices generally situated in similar geographic location. The location can include a floor, building or an entire branch office or several branch offices which connect to head quarters or another branch office via WAN/MAN. Each site is uniquely identified by its name. In case of the service provider networks the Virtual Routing and Forwarding (VRF) on a Provider Edge (PE) router or a Customer Edge (CE) routers can be defined as a site.

If a QA probe associated with the remote site matches the local site, the QA probes of the local site overrides the remote site QA probes. In such instances, NNM iSPI Performance for QA overrides the site configuration and not the thresholds configured for the site.

However, if there is no local site that matches the remote site, the QA probes are associated with the remote site.

Example








Consider a network managed in a GNM environment with branch offices 1 and 2 monitored by regional managers R1 and R2 with the global manager as G1. Consider a set of sites configured in R1 and R2, which are exported to G1. The probes obtained from R1 and R2 are consolidated in G1.








If the sites matching the remote probes are configured in G1, the QA probes of G1 override the remote site QA probes. If there is no match, the remote QA probes are available in G1.

Launching the Site Configuration Form

Perform the following steps to launch the site configuration form:

1. Log on to NNMi console using your user name and password.
You must have administrator privileges.
2. From the workspace navigation panel, select **Configuration** workspace.
3. Select **Quality Assurance Configuration Console**.
The console opens.
4. In the **Configuration** workspace, select **Site (QA Probes)**.
The Site Configuration form opens.
5. You can perform the following tasks using the Site Configuration form:

Icon	Description
 Close	Closes the Site Configuration form without saving the current configuration.
 Save	Saves the current configuration.
 Save and Close	Saves the current configuration and closes the Site Configuration form.
 Refresh	Retrieves the last saved site configuration from the database and displays the data in the Configured Sites panel of the Site Configuration form.
 Recompute Probes Associations	Associates probes with sites.
 Export	Exports sites.
 Import	Imports sites.

Icon	Description
Icons Available in the Global Settings Panel	
Enable Site Configuration	Enables to associate the configured sites to the probes.
Icons Available in the Configured Sites Tab	
 New	Adds a site
 Clone	Clones (copies) the selected site
 Open	View an existing site
 Edit	Edits an existing site
 Delete	Deletes the selected site
 Refresh	Refreshes the Configured Sites panel and displays the last saved site configurations
 Delete All	Deletes all the existing sites.

You can view the following in the **Configured Sites** panel:

Field Name	Description
Site Name	The name of the site configured.
Regional Manager	The regional manager where the sites are configured.
Order	The ordering number assigned to the site.
Node Group Rule	The node group rule configured for the site.
IP Range Rule	The IP range rule configured for the site.
Probe Name Rule	The probe name rule configured for the site.
VRF Name Rule	The VRF name rule configured for the site.

Adding Sites

To add a site, follow the steps given below:

1. [Launch the Site Configuration form.](#)
 - a. Select **Configuration workspace > Quality Assurance Configuration Console**. The configuration console opens.

- b. In the **Configuration** workspace, select **Sites/QA Groups > Site (QA Probes)**. The Site Configuration form opens.
 2. Click *** New** in the Configured Sites panel.
The Add Site Configuration form opens.
 3. Enter values for the following [site rules](#)¹:
 - a. Site Name:
Enter the name you want to assign to the site.
Site names are case sensitive. That is SiteA and Sitea are considered two different sites.
Site names must be unique. Also, it is recommended to use unique site names across the sites in a GNM environment.
Site names cannot contain ' (single quotation marks).
When you rename a site, it is identified by the new name.
 - b. Order:
A QA probe can be associated with only one source or destination site. Specify an ordering number for the site in this field to resolve conflicts in case a QA probe matches multiple sites. The NNM iSPI Performance for QA associates the QA probe with the site that has the lowest ordering number.
If you do not provide an ordering number for the site, the NNM iSPI Performance for QA assigns default ordering. Default ordering for a site is given the lowest priority.
The QA probe is associated with the site which has the **lowest** ordering in case the QA probe matches multiple sites.

Example 1

The discovered QA probe name "UDP QA probe from Site A over WAN link to SiteB" is associated with both SiteA and SiteB. The ordering number for SiteA is 1, and the ordering number for SiteB is 2. SiteA is given priority to the QA probe —UDP QA probe from Site A over WAN link to SiteB.

If a QA probe is associated with multiple sites and the ordering is the same for both sites, the weights of the [site rules](#)² are used to resolve the conflict. The weights are inherent to the site rules.

Example 2

¹Configuration associated to a site are called site rules. For example Node Group, Ordering, Test Name Pattern, etc are the site rules that are used to configure a site. The rules are prioritized inherently. The Node Group rule has the highest priority, the IP Address rule the second highest priority. Test Name Pattern rule has the third highest priority while the VRF Name rule has the lowest priority among these four rules. Note that none of these rules have any dependency to each other. In other words, while creating a site, you can specify all or any of the rules.

²Configuration associated to a site are called site rules. For example Node Group, Ordering, Test Name Pattern, etc are the site rules that are used to configure a site. The rules are prioritized inherently. The Node Group rule has the highest priority, the IP Address rule the second highest priority. Test Name Pattern rule has the third highest priority while the VRF Name rule has the lowest priority among these four rules. Note that none of these rules have any dependency to each other. In other words, while creating a site, you can specify all or any of the rules.

The discovered QA probe name "UDP QA probe from Site A over WAN link to SiteB" is associated with both SiteA and SiteB. The ordering number for both SiteA and SiteB is 1.

However, QA probe "UDP QA probe from Site A over WAN link to SiteB" matches the Node Group rule for SiteA and the QA Probe Name Pattern rule for SiteB. This QA probe is therefore associated with SiteA because the Node Group rule has a higher priority than the QA Probe Name Pattern rule.

If the inherent site rules also match for the conflicting sites, the NNM iSPI Performance for QA uses the last modified time to prioritize the sites. In this case, the QA probe is associated to the most recently configured site.

c. Node Group:

Enter the node group that you want to assign to the site.

You can classify the node groups based on their types, geographic locations etc, when you add them to a site.

The node group must be discovered by HP Network Node Manager i Software and must be already present in the NNMi database.


d. Select an NNMi tenant from the list of tenants created in NNMi.

NNMi provides a tenant named Default Tenant and assigns each newly discovered node to the Default Tenant and the Security Group attribute value configured for the Default Tenant. As an NNMi administrator, you can create new tenants and security groups. See *Configure Tenants* and *Configuring Security* in *HP Network Node Manager i Software Online Help: Help for Administrators*.

e. IP Address Range:

Type the IP address or IP address range and click  **Add** to associate an IP address or IP address range to the site. The new IP address is added to the list in the IP Address Range box. You can add IPv4 and IPv6 addresses.

Select an IP address or IP address range and click  **Delete** to remove it from the IP Address Range box.

You can click  **Delete All** to remove all the addresses listed in the IP Address Range box.

Follow the rules given below, when defining an IP address range:


- For IPv4 addresses, you can use "-" (the character hyphen) when defining a range.
Specify the range in the ascending order. The range must be from a lower value to a higher value.
- For IPV4 addresses use the wild card character "*" to specify IP addresses between 0 to 255.
- For both IPv4 and IPv6, specify an IP address range using "-" (hyphen).
- For both IPv4 and IPv6, specify the IP address range in the ascending order. For example, 16.*.*, 17.1-100.*.*.
- For IPv4, addresses such as 0.0.0.0 and 127.0.0.1 are considered as invalid.
- For IPv6 addresses, use the [standard IPv6 shorthand notation](#).

f. Probe Name Patterns:

The Probe Name Patterns box lists the QA probes associated with the node group.

By default, NNM iSPI Performance for QA populates the Probe Name Patterns box with the QA probe names associated with the node group assigned to the site.

You can associate a different QA probe with the site. Type the QA probe name patterns and

click  **Add** to associate a different group of QA probes to the site. The new QA probe name is added to the list in the Probe Name Patterns box.

You can specify a range of QA probe names using the wildcard character "?" (to replace one character) and "*" (to replace multiple characters).

The QA probe name pattern is split into three parts. Follow the rules given below, when specifying a QA probe pattern:

- If the QA probe name pattern includes both source and destination information, use a delimiter to differentiate them.

The QA probe pattern must be in the following format:

<pattern for source of the QA probe>|Delimiter| <pattern for destination of the QA probe>

- The string on the left hand side of the delimiter is considered as the source information.
- The string on the right hand side of the delimiter is considered as the destination information.

Example 1

QA Probe Name Pattern: SiteA|over|*SiteB

If you specify the delimiter between two "|" (vertical bar) characters, NNM iSPI Performance for QA considers the QA probe names that contain the word "over". It also considers the following:

- The source information on the left hand side of the delimiter "over" must contain the string "SiteA".
- The destination information on the right hand side of the delimiter "over" must contain the string "SiteB" preceding any number of characters.

If you have two QA probes named "UDP QA probe From SiteA over Provider WAN to SiteB" and "ICMP QA probe From SiteA over Provider WAN to SiteB", NNM iSPI Performance for QA retrieves both QA probe names.

Example 2

QA Probe Name Pattern: remote???|to|central*

This QA probe pattern retrieves QA probe names that match the following criteria:

- The source information on the left hand side of the delimiter "to" must contain the string "remote", followed by three characters.
- The destination information on the right hand side of the delimiter "to" must contain the string "central" followed by any number of characters.

If you have QA probes named "remoteABC to centralHQ", and "remote123 to centralSite", NNM iSPI Performance for QA retrieves both the QA probe names.

- You cannot include blank spaces in QA probe name pattern, but you must enter the wild card "*" (asterisk) wherever required. See the example below:


Example 3

QA Probe Name Pattern: *|to|test_location

The wildcard "*" must be entered in the source information if you want to leave the source information blank, and you want to retrieve the QA probe names of the destination test_location. In this example, the NNM iSPI Performance for QA does not check for the source information, and it retrieves all the probes with the destination test_location. Use this expression if you want to configure a site with all the probes that have test_location as the destination.


Note: The above expression also retrieves probes that include the term "to" in the probe source name but not do not have their destination set to test_location.

Select a QA probe name and click  **Delete** to remove it from the Probe Name Patterns box.

You can click  **Delete All** to select all the QA probes listed in the Probe Name Patterns box and remove them from the Probe Name Patterns box.


g. VRF Wildcards:

If your site is associated with a Virtual Private Network (VPN), NNM iSPI Performance for QA populates the VRF Wildcards box with the available VRF ranges. Make sure that the VRF name is associated with the IP address rule that is defined.




You can associate a different VRF range with the site. Type the VRF range and click  **Add** to associate another VRF range to the site. The new VRF range is added to the list in the VRF Wildcards box.


You can specify a range of VRF using the wildcard character "?" (to replace one character) and "*" (to replace multiple characters).

Select a VRF range and click  **Delete** to remove it from the VRF Wildcards box.

You can click  **Delete All** to remove all the VRF ranges listed in the VRF Wildcards box.

4. You can also perform the following actions:

Icon	Description
 Close	Closes the Add Site Configuration form without saving the site information you have entered.
 Save	Saves the new site information.
 Save and Close	Saves the site information and closes the Add Site Configuration form.


5. Click  **Refresh** in the Configured Sites panel to view the changes.

6. On the Site Configuration form, click  **Save**.

Note: On the Site Configuration form, select the **Enable Site Configuration** check box to associate probes with the sites in the next configuration poll. For more information about associating probes with sites, see "[Associating Probes with Sites](#)" on page 192.

Editing Sites

To edit an existing site:

1. [Launch the Site Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Sites/QA Groups** > **Site (QA Probes)**. The Site Configuration form opens.
 2. Select a site in the **Configured Sites** tab and click  **Edit**.
The Edit Site Configuration form opens.
From the global manager, you can only view the remote sites and not edit them.
 3. Update the following values as required:
 - a. **Site Name:**
Enter the name you want to assign to the site.

Site names are case sensitive. That is SiteA and Sitea are considered two different sites.

Site names must be unique. Also, it is recommended to use unique site names across the sites in a GNM environment.

Site names cannot contain ' (single quotation marks).

When you rename a site, it is identified by the new name.
 - b. **Ordering:**
A QA probe can be associated with only one source or destination site. Specify an ordering number for the site in this field to resolve conflicts in case a QA probe matches multiple sites. The NNM iSPI Performance for QA associates the QA probe with the site that has the lowest ordering number.

If you do not provide an ordering number for the site, the NNM iSPI Performance for QA assigns default ordering. Default ordering for a site is given the lowest priority.

The QA probe is associated with the site which has the **lowest** ordering in case the QA probe matches multiple sites.
- Example 1**
- The discovered QA probe name "UDP QA probe from Site A over WAN link to SiteB" is associated with both SiteA and SiteB. The ordering number for SiteA is 1, and the ordering number for SiteB is 2. SiteA is given priority to the QA probe —UDP QA probe from Site A over WAN link to SiteB.

If a QA probe is associated with multiple sites and the ordering is the same for both sites, the weights of the [site rules](#)¹ are used to resolve the conflict. The weights are inherent to the site rules.

Example 2

The discovered QA probe name "UDP QA probe from Site A over WAN link to SiteB" is associated with both SiteA and SiteB. The ordering number for both SiteA and SiteB is 1.

However, QA probe "UDP QA probe from Site A over WAN link to SiteB" matches the Node Group rule for SiteA and the QA Probe Name Pattern rule for SiteB. This QA probe is therefore associated with SiteA because the Node Group rule has a higher priority than the QA Probe Name Pattern rule.

If the inherent site rules also match for the conflicting sites, the NNM iSPI Performance for QA uses the last modified time to prioritize the sites. In this case, the QA probe is associated to the most recently configured site.

This field displays "Default" if you have not specified a value for this field while creating the site. By default the NNM iSPI Performance for QA assigns a site the lowest ordering value.

c. Node Group:

Enter the node group that you want to assign to the site.


You can classify the node groups based on their types, geographic locations etc, when you add them to a site.

The node group must be discovered by HP Network Node Manager i Software and must be already present in the NNMi database.

d. Select an NNMi tenant from the list of tenants created in NNMi.


NNMi provides a tenant named Default Tenant and assigns each newly discovered node to the Default Tenant and the Security Group attribute value configured for the Default Tenant. As an NNMi administrator, you can create new tenants and security groups. See *Configure Tenants* and *Configuring Security* in *HP Network Node Manager i Software Online Help: Help for Administrators*.

e. IP Address Range:

Type the IP address or IP address range and click  **Add** to associate an IP address or IP address range to the site. The new IP address is added to the list in the IP Address Range box. You can add IPv4 and IPv6 addresses.

Select an IP address or IP address range and click  **Delete** to remove it from the IP Address Range box.

¹Configuration associated to a site are called site rules. For example Node Group, Ordering, Test Name Pattern, etc are the site rules that are used to configure a site. The rules are prioritized inherently. The Node Group rule has the highest priority, the IP Address rule the second highest priority. Test Name Pattern rule has the third highest priority while the VRF Name rule has the lowest priority among these four rules. Note that none of these rules have any dependency to each other. In other words, while creating a site, you can specify all or any of the rules.

You can click  **Delete All** to remove all the addresses listed in the IP Address Range box.

Follow the rules given below, when defining an IP address range:


- For IPv4 addresses, you can use "-" (the character hyphen) when defining a range. Specify the range in the ascending order. The range must be from a lower value to a higher value.
- For IPV4 addresses use the wild card character "*" to specify IP addresses between 0 to 255.
- For both IPv4 and IPv6, specify an IP address range using "-" (hyphen).
- For both IPv4 and IPv6, specify the IP address range in the ascending order. For example, 16.*.* , 17.1-100.*.*.
- For IPv4, addresses such as 0.0.0.0 and 127.0.0.1 are considered as invalid.
- For IPv6 addresses, use the [standard IPv6 shorthand notation](#).

f. Probe Name Patterns:

The Probe Name Patterns box lists the QA probes associated with the node group.

By default, NNM iSPI Performance for QA populates the Probe Name Patterns box with the QA probe names associated with the node group assigned to the site.

You can associate a different QA probe with the site. Type the QA probe name patterns and click

 **Add** to associate a different group of QA probes to the site. The new QA probe name is added to the list in the Probe Name Patterns box.

You can specify a range of QA probe names using the wildcard character "?" (to replace one character) and "*" (to replace multiple characters).

The QA probe name pattern is split into three parts. Follow the rules given below, when specifying a QA probe pattern:

- If the QA probe name pattern includes both source and destination information, use a delimiter to differentiate them.

The QA probe pattern must be in the following format:

<pattern for source of the QA probe>|Delimiter| <pattern for destination of the QA probe>

- The string on the left hand side of the delimiter is considered as the source information.
- The string on the right hand side of the delimiter is considered as the destination information.

Example 1

QA Probe Name Pattern: SiteA|over|*SiteB

If you specify the delimiter between two "|" (vertical bar) characters, NNM iSPI Performance for QA considers the QA probe names that contain the word "over". It also considers the following:

- The source information on the left hand side of the delimiter "over" must contain the string "SiteA".
- The destination information on the right hand side of the delimiter "over" must contain the string "SiteB" preceding any number of characters.

If you have two QA probes named "UDP QA probe From SiteA over Provider WAN to SiteB" and "ICMP QA probe From SiteA over Provider WAN to SiteB", NNM iSPI Performance for QA retrieves both QA probe names.

Example 2

QA Probe Name Pattern: remote???|to|central*

This QA probe pattern retrieves QA probe names that match the following criteria:

- The source information on the left hand side of the delimiter "to" must contain the string "remote", followed by three characters.
- The destination information on the right hand side of the delimiter "to" must contain the string "central" followed by any number of characters.

If you have QA probes named "remoteABC to centralHQ", and "remote123 to centralsite", NNM iSPI Performance for QA retrieves both the QA probe names.

- You cannot include blank spaces in QA probe name pattern, but you must enter the wild card "*" (asterisk) wherever required. See the example below:


Example 3

QA Probe Name Pattern: *|to|test_location

The wildcard "*" must be entered in the source information if you want to leave the source information blank, and you want to retrieve the QA probe names of the destination test_location. In this example, the NNM iSPI Performance for QA does not check for the source information, and it retrieves all the probes with the destination test_location. Use this expression if you want to configure a site with all the probes that have test_location as the destination.


Note: The above expression also retrieves probes that include the term "to" in the probe source name but do not have their destination set to test_location.

Select a QA probe name and click  **Delete** to remove it from the Probe Name Patterns box.

You can click  **Delete All** to select all the QA probes listed in the Probe Name Patterns box and remove them from the Probe Name Patterns box.


g. VRF Wildcards

If your site is associated with a Virtual Private Network (VPN), NNM iSPI Performance for QA populates the VRF Wildcards box with the available VRF ranges. Make sure that the VRF name is associated with the IP address rule that is defined.




You can associate a different VRF range with the site. Type the VRF range and click  **Add** to associate another VRF range to the site. The new VRF range is added to the list in the VRF Wildcards box.

You can specify a range of VRF using the wildcard character "?" (to replace one character) and "*" (to replace multiple characters).

Select a VRF range and click  **Delete** to remove it from the VRF Wildcards box.

You can click  **Delete All** to remove all the VRF ranges listed in the VRF Wildcards box.

4. You can perform the following actions:




Icons	Description
 Close	Closes the Edit Site Configuration form without saving the site information you have entered.
 Save	Saves the new site information.
 Save and Close	Saves the site information and closes the Edit Site Configuration form.

5. Click  **Refresh** in the Configured Sites panel to view the changes.

6. On the Site Configuration form, click  **Save**.

Deleting Sites

To delete an existing site:

1. [Launch the Site Configuration form](#).
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Sites/QA Groups** > **Site (QA Probes)**. The Site Configuration form opens.
2. Select a site in the **Configured Sites** panel and click  **Delete**.
or
Click  **Delete All** to delete all the sites.
3. Click  **Refresh** in the **Configured Sites** panel to view the changes.

The QA probe associations for the site are deleted automatically once you delete a site. You do not need to recompute the QA probe associations after deleting a site.

In a GNM environment, the global manager cannot delete [Remote Sites](#)¹. The sites deleted at the regional manager are propagated to the global manager. In case, the synchronization takes more time, you can run the following commands to trigger synchronization:

To synchronize the deletion of sites at regional manager to the global manager:

```
nmsqasiteconfigutil -synchronize <regional manager name>
```


To synchronize the deletion of sites at all regional managers to the global manager:

¹Sites exported from the regional manager to the global manager are known as Remote Sites.

```
nmsqasiteconfigutil -synchronize all
```

Viewing Sites

To view a site configuration:

1. [Launch the Site Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Sites/QA Groups** > **Site (QA Probes)**. The Site Configuration form opens.
2. Select a site in the **Configured Sites** panel and click  **Open**.


The View Site Configuration Details form opens.

You can view the following details:

Field Name	Description
Site Name	The name of the site.
Order	The ordering number for the site. This field displays "Default" if you have not specified a value for this field when creating the site.
Regional Manager	The name of the Regional Manager where the site was configured.
Node Group	The node group assigned to the site.
Tenant	The NNMi tenant name associated with the site.
IP Address Range	The set of IPv4 or IPv6 addresses associated with the site.
Probe Name Pattern	The QA probes or the Probe Name patterns of the QA probes that are associated with the site.
VRF Wildcards	The VRF name associated with the site.

Exporting Sites

To export the existing site configurations to an XML file:

1. [Launch the Site Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Sites/QA Groups** > **Site (QA Probes)**. The Site Configuration form opens.
2. Click  **Export**.
3. Enter the file name where you want to export the existing site configuration in the user prompt

dialog.

You must enter the file name with full path information. For example, C:\temp\site_conf.xml

If you enter the XML file name without entering the absolute path, by default the file is saved in the following directory of the NNMi management server where NNM iSPI Performance for QA is installed:

Linux: \$NnmDataDir/shared/qa/conf

Windows : %NnmDataDir%\shared\qa\conf

4. Click **OK** in the user prompt dialog.

You can also export the existing site configuration using the following command line utility:

Linux: \$NnmInstallDir/bin/nmsqasiteconfigutil.ovpl -u <username> -p <password> -export <filename>

Windows: %NnmInstallDir%\bin\nmsqasiteconfigutil.ovpl -u <username> -p <password> -export <filename>

If the site export fails, check the following log files:

Linux: \$NnmDataDir/log/qa/qa.log


Windows: %NnmDataDir%\log\qa\qa.log

Note: You can export local sites, but you cannot export remote sites.

Note: -u <username> -p <password> are optional parameters.

Importing Sites

To import site configurations from an XML file:

1. [Launch the Site Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Sites/QA Groups** > **Site (QA Probes)**. The Site Configuration form opens.
2. Click  **Import**.
 - c. In the user prompt dialog, enter the file name from where you want to import the site configuration information.

You must enter the file name with full path information; for example, C:\temp\site_conf.xml

Note: You can import the sites configured in the previous version of NNM iSPI Performance for QA as well.

4. Click **OK** in the user prompt dialog.

If a site is already defined and displayed in the Configured Sites panel, the import utility does not import the configuration information for this site from the XML file.

You can also import site configuration information using the following command line utility:

Linux: `$NnmInstallDir/bin/nmsqasiteconfigutil.ovpl -u <username> -p <password> -import <filename>`

Windows: `%NnmInstallDir%\bin\nmsqasiteconfigutil.ovpl -u <username> -p <password> -import <filename>`

If the site import fails, check the following log files:

Linux: `$NnmDataDir/log/qa/qa.log`


Windows: `%NnmDataDir%\log\qa\qa.log`

Note: `-u <username> -p <password>` are optional parameters.

Associating Probes with Sites

To associate probes with the new or updated sites, do one of the following:

- On the Site Configuration form, select the **Enable Site Configuration** check box at the time of creating or updating sites and click **Save**. Selecting this check box associates probes with the sites in the next configuration poll. If you do not select this check box, sites still get created or updated but probes do not get associated with them.

- On the Site Configuration form, click the  **Recompute Probes Associations** button to associate probes with the new or updated sites immediately.

- Use the following command line utility to associate probes with the new or updated sites immediately:

- **Linux:** `/opt/OV/bin/nmsqasiteconfigutil.ovpl -u <username> -p <password> -recompute`

- **Windows:** `%NnmInstallDir%\bin\nmsqasiteconfigutil.ovpl -u <username> -p <password> -recompute`

By default, the `/opt/OV/bin` and `%NnmInstallDir%is <drive>:\Program Files(x86)\HP\HP BTO Software\`

If the re-computation does not occur due to an internal error, you can run the following command to reset the internal queue and the gateway flag to allow subsequent probe associations:

`nmsqasiteconfigutil.ovpl -resetrecomputeQ`

Note: `-u <username> -p <password>` are optional parameters.

User Scenario

The head office of an organization is connected to its branch office via WAN links. To monitor the network performances of the branch office, a new site is created using the NNM iSPI Performance for QA Site Configuration form. The new site contains the following parameters:

Site Name: SiteA

Order: 1

Node Group: Routers

IP Address Range: 17.1-100.*.*

Probe Name Patterns: *SiteA|to|Central

VRF Wildcards: None

Later, you want to add the following QA probe name patterns to SiteA:

- SiteA??|to|*Central
- SiteA*|over|Central*


Also, you want to add the following VRF groups:

- VRF 1-SiteA
- VRF 2-SiteA

After the site is reconfigured, the QA probes matching the specified QA probe patterns for the node group "Routers" are associated with SiteA in the next configuration poll. Use the **Recompute Probes Associations** button to associate the QA probes to the new or updated sites immediately.

Cloning (Copying) Site Configurations

To clone the existing configuration for a selected site:

1. [Launch the Site Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Sites/QA Groups** > **Site (QA Probes)**. The Site Configuration form opens.
2. Select the site you want to copy.
2. Click  **Clone** in the Configured Sites panel.
The Edit Site Configuration form opens.
3. You can update values for the following [site rules](#)¹:
 - a. Site Name:
Enter the name you want to assign to the site.
Site names are case sensitive. That is SiteA and Sitea are considered two different sites.
Site names must be unique. Also, it is recommended to use unique site names across the sites in a GNM environment.
Site names cannot contain ' (single quotation marks).

¹Configuration associated to a site are called site rules. For example Node Group, Ordering, Test Name Pattern, etc are the site rules that are used to configure a site. The rules are prioritized inherently. The Node Group rule has the highest priority, the IP Address rule the second highest priority. Test Name Pattern rule has the third highest priority while the VRF Name rule has the lowest priority among these four rules. Note that none of these rules have any dependency to each other. In other words, while creating a site, you can specify all or any of the rules.

When you rename a site, it is identified by the new name.

b. Order:

A QA probe can be associated with only one source or destination site. Specify an ordering number for the site in this field to resolve conflicts in case a QA probe matches multiple sites. The NNM iSPI Performance for QA associates the QA probe with the site that has the lowest ordering number.

If you do not provide an ordering number for the site, the NNM iSPI Performance for QA assigns default ordering. Default ordering for a site is given the lowest priority.

The QA probe is associated with the site which has the **lowest** ordering in case the QA probe matches multiple sites.

Example 1

The discovered QA probe name "UDP QA probe from Site A over WAN link to SiteB" is associated with both SiteA and SiteB. The ordering number for SiteA is 1, and the ordering number for SiteB is 2. SiteA is given priority to the QA probe —UDP QA probe from Site A over WAN link to SiteB.

If a QA probe is associated with multiple sites and the ordering is the same for both sites, the weights of the [site rules](#)¹ are used to resolve the conflict. The weights are inherent to the site rules.

Example 2

The discovered QA probe name "UDP QA probe from Site A over WAN link to SiteB" is associated with both SiteA and SiteB. The ordering number for both SiteA and SiteB is 1.

However, QA probe "UDP QA probe from Site A over WAN link to SiteB" matches the Node Group rule for SiteA and the QA Probe Name Pattern rule for SiteB. This QA probe is therefore associated with SiteA because the Node Group rule has a higher priority than the QA Probe Name Pattern rule.

If the inherent site rules also match for the conflicting sites, the NNM iSPI Performance for QA uses the last modified time to prioritize the sites. In this case, the QA probe is associated to the most recently configured site.

c. Node Group:

Enter the node group that you want to assign to the site.

You can classify the node groups based on their types, geographic locations etc, when you add them to a site.

The node group must be discovered by HP Network Node Manager i Software and must be already present in the NNMi database.


d. Select an NNMi tenant from the list of tenants created in NNMi.

NNMi provides a tenant named Default Tenant and assigns each newly discovered node to the Default Tenant and the Security Group attribute value configured for the Default Tenant. As an


¹Configuration associated to a site are called site rules. For example Node Group, Ordering, Test Name Pattern, etc are the site rules that are used to configure a site. The rules are prioritized inherently. The Node Group rule has the highest priority, the IP Address rule the second highest priority. Test Name Pattern rule has the third highest priority while the VRF Name rule has the lowest priority among these four rules. Note that none of these rules have any dependency to each other. In other words, while creating a site, you can specify all or any of the rules.

NNMi administrator, you can create new tenants and security groups. See *Configure Tenants* and *Configuring Security* in *HP Network Node Manager i Software Online Help: Help for Administrators*.

e. IP Address Range:

Type the IP address or IP address range and click  **Add** to associate an IP address or IP address range to the site. The new IP address is added to the list in the IP Address Range box. You can add IPv4 and IPv6 addresses.

Select an IP address or IP address range and click  **Delete** to remove it from the IP Address Range box.

You can click  **Delete All** to remove all the addresses listed in the IP Address Range box.

Follow the rules given below, when defining an IP address range:


- For IPv4 addresses, you can use "-" (the character hyphen) when defining a range. Specify the range in the ascending order. The range must be from a lower value to a higher value.
- For IPv4 addresses use the wild card character "*" to specify IP addresses between 0 to 255.
- For both IPv4 and IPv6, specify an IP address range using "-" (hyphen).
- For both IPv4 and IPv6, specify the IP address range in the ascending order. For example, 16.*.*, 17.1-100.*.*.
- For IPv4, addresses such as 0.0.0.0 and 127.0.0.1 are considered as invalid.
- For IPv6 addresses, use the [standard IPv6 shorthand notation](#).

f. Probe Name Patterns:

The Probe Name Patterns box lists the QA probes associated with the node group.

By default, NNM iSPI Performance for QA populates the Probe Name Patterns box with the QA probe names associated with the node group assigned to the site.

You can associate a different QA probe with the site. Type the QA probe name patterns and

click  **Add** to associate a different group of QA probes to the site. The new QA probe name is added to the list in the Probe Name Patterns box.

You can specify a range of QA probe names using the wildcard character "?" (to replace one character) and "*" (to replace multiple characters).

The QA probe name pattern is split into three parts. Follow the rules given below, when specifying a QA probe pattern:

- If the QA probe name pattern includes both source and destination information, use a delimiter to differentiate them.

The QA probe pattern must be in the following format:

<pattern for source of the QA probe>|Delimiter| <pattern for destination of the QA probe>

- The string on the left hand side of the delimiter is considered as the source information.
- The string on the right hand side of the delimiter is considered as the destination information.

Example 1

QA Probe Name Pattern: SiteA|over|*SiteB

If you specify the delimiter between two "|" (vertical bar) characters, NNM iSPI Performance for QA considers the QA probe names that contain the word "over". It also considers the following:

- The source information on the left hand side of the delimiter "over" must contain the string "SiteA".
- The destination information on the right hand side of the delimiter "over" must contain the string "SiteB" preceding any number of characters.

If you have two QA probes named "UDP QA probe From SiteA over Provider WAN to SiteB" and "ICMP QA probe From SiteA over Provider WAN to SiteB", NNM iSPI Performance for QA retrieves both QA probe names.

Example 2

QA Probe Name Pattern: remote???|to|central*

This QA probe pattern retrieves QA probe names that match the following criteria:

- The source information on the left hand side of the delimiter "to" must contain the string "remote", followed by three characters.
- The destination information on the right hand side of the delimiter "to" must contain the string "central" followed by any number of characters.

If you have QA probes named "remoteABC to centralHQ", and "remote123 to centralsite", NNM iSPI Performance for QA retrieves both the QA probe names.

- You cannot include blank spaces in QA probe name pattern, but you must enter the wild card "*" (asterisk) wherever required. See the example below:


Example 3

QA Probe Name Pattern: *|to|test_location

The wildcard "*" must be entered in the source information if you want to leave the source information blank, and you want to retrieve the QA probe names of the destination test_location. In this example, the NNM iSPI Performance for QA does not check for the source information, and it retrieves all the probes with the destination test_location. Use this expression if you want to configure a site with all the probes that have test_location as the destination.


Note: The above expression also retrieves probes that include the term "to" in the probe source name but not do not have their destination set to test_location.

Select a QA probe name and click  **Delete** to remove it from the Probe Name Patterns box.

You can click  **Delete All** to select all the QA probes listed in the Probe Name Patterns box and remove them from the Probe Name Patterns box.


- g. VRF Wildcards:

If your site is associated with a Virtual Private Network (VPN), NNM iSPI Performance for QA populates the VRF Wildcards box with the available VRF ranges. Make sure that the VRF name is associated with the IP address rule that is defined.




You can associate a different VRF range with the site. Type the VRF range and click  **Add** to associate another VRF range to the site. The new VRF range is added to the list in the VRF Wildcards box.

You can specify a range of VRF using the wildcard character "?" (to replace one character) and "*" (to replace multiple characters).

Select a VRF range and click  **Delete** to remove it from the VRF Wildcards box.

You can click  **Delete All** to remove all the VRF ranges listed in the VRF Wildcards box.

4. You can perform the following actions::

Icons	Description
 Close	Closes the Edit Site Configuration form without saving the site information you have entered.
 Save	Saves the new site information.
 Save and Close	Saves the site information and closes the Edit Site Configuration form.

5. Click  **Refresh** in the Configured Sites panel to view the changes.

Troubleshooting Site Configuration Error Messages

The error log files are available in the following directory:

Linux: `./var/opt/OV/log/qa/qa.log`

Windows: `%NnmDataDir%\log\qa\qa.log`

[Failed to create the site. Please check the log files.](#)

May occur for various reasons. Some of the reasons are as follows:

- If a site with the same name already exists. NNM iSPI Performance for QA recognizes a site by its name. Site names must be unique.
- If the IP address range is not valid.
- If the node group you specified does not exist in the NNMi database.

Reason and Resolution

Check any of the following log files:

Linux: `./var/opt/OV/log/qa/qa.log`

Windows: %NnmDataDir%\log\qa\qa.log

Invalid Probe Name Pattern

Occurs under any of the following circumstances:

- If the Probe Name Patterns field in the Add Site Configuration form contains any illegal character.
- If the Probe Name Patterns field in the Add Site Configuration form does not contain the delimiter "|" (VERTICAL BAR).

Reason and Resolution

- Avoid using '(SINGLE QUOTE) as a probe name pattern. NNM iSPI Performance for QA does not accept this character in a probe name pattern.
- You must use the delimiter to separate the source information and the destination information for the QA probe name pattern.

Order cannot be less than 0.

Occurs when you specify a negative site ordering. For example, -1 (MINUS ONE).

Reason and Resolution

The minimum site ordering accepted is 0 (ZERO).

Invalid Site Name

Occurs if the Site Name field in the Add Site Configuration form contains any illegal character.

Reason and Resolution

Avoid using '(SINGLE QUOTE) as a site name. NNM iSPI Performance for QA does not accept this character in a site name.

Failed to import the site configuration. Please check the log files.

Occurs under any of the following circumstances:

- If the import file does not exist in the path you entered.
- If a site is already defined and displayed in the Configured Sites panel.

Reason and Resolution

NNM iSPI Performance for QA imports the site configuration from an XML file. If the file path is not correct, NNM iSPI Performance for QA fails to import the configuration information.

Also the import utility does not import the site configuration if the configuration is unchanged since the last import

Check any of the following log files:

Linux: ./var/opt/OV/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

[Failed to export the site configuration. Please check the log files.](#)

Occurs if the export file path that you entered is incorrect.

Reason and Resolution

NNM iSPI Performance for QA exports the site configuration to an XML file. If the file path is not correct, NNM iSPI Performance for QA fails to export the configuration information.

Check any of the following log files:

Linux: `./var/opt/OV/log/qa/qa.log`

Windows: `%NnmDataDir%\log\qa\qa.log`

[Site name already exists, cannot add new site](#)

Occurs when you try to save site configurations with a site name that already exists

Reason and Resolution

You must enter a unique name for the site in the Site Configuration form. Site names are unique for a manager or NNMi management server.

[Invalid Node Group Name cannot add new site](#)

Occurs when you enter an invalid Node Group Name in the Site Configuration form.

Reason and Resolution

Enter a valid node group name

[Update failed, invalid node group specified](#)

Occurs when you try to save the site details in the Edit Site Configuration form, and you specified an invalid node group

Reason and Resolution

You must enter a valid node group configured in NNMi

[Unable to write/retrieve data from the server](#)

Occurs due to any exceptions raised while retrieving data from the server

Reason and Resolution

Check any of the following log files:

Linux: `./var/opt/OV/log/qa/qa.log`

Windows: `%NnmDataDir%\log\qa\qa.log`

Chapter 6: Configuring QA Groups

In a large enterprise network, you can have many elements of NNM iSPI Performance for QA. Without a grouping and filtering mechanism, managing and monitoring these elements can become time consuming and cumbersome. NNM iSPI Performance for QA enables you to group NNM iSPI Performance for QA elements based on a common feature. You can use the QA groups to perform the following tasks:

- Configure entity thresholds as a group¹
- View the entities based on the groups²
- Configure polling frequency³

One NNM iSPI Performance for QA element can be part of multiple QA Groups.

You can group the NNM iSPI Performance for QA elements based on various attributes.

Note: You cannot create a QA Group with more than nine attributes.

Grouping attributes for QA Probe Elements:

- Probe Name
- Probe Owner Name
- Probe Type
- Probe ToS
- Source Host
- Source Address
- Target Address
- Destination Host
- VRF Name
- Source Site
- Destination Site
- Node Group Name

Note: After creating a new QA group using a newly created node group, wait for 30 minutes, and then click **Apply Now** in the QA Groups panel or run a discovery to ensure successful association of probes with the new QA group. For information about running an on-demand discovery, see "[On-Demand Discovery](#)" on page 149.

¹You can configure entity thresholds based on the QA groups. When you configure a threshold for a QA group, NNM iSPI Performance for QA applies the threshold to all the entities that belong to the QA group.

²You can view the state of the entities based on the QA group.

³You can configure the polling frequency based on the QA groups. You can apply a specific polling frequency to all the entities that belong to the QA group.

Grouping attributes for QoS Elements:

- Policy name (NNM iSPI Performance for QA includes the parent policy in the group, if the policy is a child policy)
- Action Type
- Node on which the policy is hosted
- Policy Direction
- Interface Name (ifName)
- Interface Type (ifType)
- Interface Alias (ifAlias)
- Interface Description (ifDescr)
- Traffic Class Name
- Node group on which the policy is hosted

Note: After creating a new QA group using a newly created node group, wait for 30 minutes, and then click **Apply Now** in the QA Groups panel or run a discovery to ensure successful association of QoS elements with the new QA group. For information about running an on-demand discovery, see ["On-Demand Discovery" on page 149](#).


Grouping attributes for Ping Latency Pair Elements:

- Source Host Name
- Destination Host Name
- Source Interface Name (ifName)
- Destination Interface Name (ifName)
- Source Interface Type (ifType)
- Destination Interface Type (ifType)
- Source Interface Alias (ifAlias)
- Destination Interface Alias (ifAlias)
- Source Address
- Destination Address
- Source in Node Group

Adding QA Groups

To add a new QA Group:

1. [Launch the QA Groups Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Sites/QA Groups** > **QA Group**. The QA Groups Configuration form opens.

2. Click  **New** in the **Configured QA Groups** tab. The Add QA Group form opens.
3. Specify the following to configure the QA Group settings:

Field Name	Description
Name	The name of the QA Group. The name should be unique.
Description	<p>A brief description of the QA Group. For example, you can mention "Probes for VoIP", if you want to group all VoIP probes.</p> <p>Note: Do not use the & and < characters in the description.</p>
Type	<p>The type of the QA Group. The valid QA Group types are QA Probes, Ping Latency, and CBQoS.</p> <p>Select a type for the new QA group before you continue creating the QA group filters.</p>
Tenant	<p>The tenant name to which the QA group belongs to.</p> <p>If the value is left blank, NNMi assigns a tenant named Default Tenant. As an NNMi administrator, you can create new tenants and security groups. For more information, See <i>Configure Tenants and Configuring Security</i> in <i>HP Network Node Manager i Software Online Help: Help for Administrators</i>.</p>
Polling Interval	<p>The applicable polling interval for all the members of the QA group, in seconds.</p> <p>Note: For QoS entities and probes, you cannot use a polling interval that is less than 1 minute.</p> <ul style="list-style-type: none"> • For QoS entities (interfaces/actions), if the value remains zero, the polling interval of the QA Group is the default value, which is 300 seconds. • For QA probes, if the value remains zero, the polling interval is the default frequency of the probe. <p>If a QoS entity is a member of multiple QA groups, then it's polling frequency is that of the QA group with the lowest polling interval.</p> <p>If a QA probe is a member of multiple QA groups, then the polling frequency of the probe is that of the QA group which has the lowest polling interval. The probe-specific frequency overrides the QA group polling frequency only if the probe-specific frequency is higher than the QA group polling frequency.</p> <p>To configure the polling frequency of the QA Probes/QoS entities that are not part of any QA group, see "Configuring Polling " on page 311.</p>
Filter Editor	<p>You can create a QA group based on the Filter Editor expression created with different attributes of the NNM iSPI Performance for QA Elements. Note that the attributes listed for the Filter Editor differ based on the type of the QA group selected. You can define the Filter Editor expression with a single condition or combine multiple conditions using the Boolean Operators, AND and OR.</p>

Field Name	Description
	To define the Filter Editor expression, you must first add the Boolean operators and then add the conditions.

To add the Boolean operators: Use the [Mapping buttons](#) to [insert](#)¹, [append](#)², and [replace](#)³ Boolean Operators based on the rule that you want to create.

Button	Description
AND	Inserts the AND Boolean Operator at the selected cursor location.
OR	Inserts the OR Boolean Operator at the current cursor location.
DELETE	Deletes the selected Boolean Operator. If the Boolean Operator is selected, all the conditions associated with the Boolean Operator are deleted.

Note: See the condition expression displayed under Filter string to see the logic of the expression as it is created.

[Click here](#) for more information about using the Boolean Operators.

- Add your highest level Boolean operator first.
- The AND and OR Boolean Operators must contain at least two conditions.
- Add each additional Boolean Operator before adding the condition to which it applies.
- Place the cursor on the Boolean Operator that you want to append to or replace.

To add a condition: Use the [rule components](#) to [insert](#)⁴, [append](#)⁵, and [replace](#)⁶ a condition.

Component	Description
Attribute	The attribute on which you want NNM iSPI Performance for QA to filter the probes. The listed attributes depend on the type of the QA Group selected.

Note: You cannot create a QA Group with more than nine attributes.

¹Adds the current Boolean Operator to the beginning of the selected Boolean Operator within the Filter String.

²Adds the current Boolean Operator to the end of the selected Boolean Operator within the Filter String.

³Replaces the selected Boolean Operator with the current Boolean Operator within the Filter String.

⁴Adds the current condition (Attribute, Operator, and Value) to the beginning of the conditions already added to the selected boolean operator.

⁵Adds the current condition (Attribute, Operator, and Value) to the end of the conditions already added to the selected boolean operator.

⁶Replaces the selected condition with the current condition within the Filter String.



Component	Description
Operator	The operator that establishes the relationship between the Attribute and Value.
Value	The value that completes the criteria required to define the condition.

Note: It is recommended to group the QA probes with millisecond precision value and microsecond precision value into separate QA groups.

[Click here](#) for an example for defining the condition expression.

((Probe owner name = Admin1 OR Probe owner name = Admin2) AND Node group name = Router)

To add the Filter Editor expression above, after you are in the Filter Editor section, follow these steps:

1. Click **AND**.
2. Click **OR**.
3. Select the OR you just added to the expression.
4. In the Attribute field, select **Probe owner name**.
5. In the Operator field, select =.
6. In the Value field, enter **Admin1**.
7. Click **Insert**.
8. In the Attribute field, select **Probe owner name**.
9. In the Operator field, select =.
10. In the Value field, enter **Admin2**.
11. Click **Append/Insert**.
12. Select the AND that you added previously to the expression.
13. In the Attribute field, select **Node group name**.
14. In the Operator field, select =.
15. In the Value field, enter **Router**.
16. Click **Append**.
17. Click  **Save** or  **Save and Close**.


After you configure the QA Group, you can view the configured QA group details in the QA Groups panel.

The configured QA Group is discovered in the inventory view by clicking **Apply Now** in the QA Groups panel, or during the next discovery cycle of the nodes.

Editing QA Groups

To edit the existing QA Groups:

1. [Launch the QA Groups Configuration form](#).
 - a. Select **Configuration workspace > Quality Assurance Configuration Console**. The

- configuration console opens.
- b. In the **Configuration** workspace, select **Sites/QA Groups > QA Group**. The QA Groups Configuration form opens.
2. Select a configured QA Group you want to modify, and Click  **Edit** in the **Configured QA Groups** tab. The Edit QA Group form opens.
 3. You can update one or more fields in the QA Group settings:

Field Name	Description
Name	The name of the QA Group. The name should be unique.
Description	A brief description for the QA Group. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 5px;">Note: Do not use the & and < characters in the description.</div>
Tenant	The tenant name to which the QA group belongs to. If the value is left blank, NNMI assigns 'Default Tenant' as the tenant name. As an NNMI administrator, you can create new tenants and security groups. For more information, see <i>Configure Tenants and Configuring Security in HP Network Node Manager i Software Online Help: Help for Administrators</i> .
Polling Interval	The applicable polling interval for all the members of the QA group, in seconds. For QA probes: <ul style="list-style-type: none"> • If the value remains zero, the polling interval is the probe-specific frequency. • If a QA probe is a member of multiple QA groups, then the polling frequency of the probe is that of the QA group which has the lowest polling interval. The probe-specific frequency overrides the QA group polling frequency only if the probe-specific frequency is higher than the QA group polling frequency. For QoS interfaces/actions: <ul style="list-style-type: none"> • If the value remains zero, the polling interval of the QA Group is the default value, which is 300 seconds. • If a QoS entity is a member of multiple QA groups, then it's polling frequency is that of the QA group with the lowest polling interval. To configure the polling frequency of the QA Probes/QoS entities that are not part of any QA group, see " Configuring Polling " on page 311.

The Type of the QA Group cannot be changed.

To edit the boolean operators: Use the [mapping buttons](#) to [insert](#)¹, [append](#)², and [replace](#)³ boolean operators based on the rule that you want to create.

Button	Description
AND	Inserts the AND Boolean Operator at the selected cursor location.
OR	Inserts the OR Boolean Operator at the current cursor location.
DELETE	Deletes the selected Boolean Operator. If the Boolean Operator is selected, all the conditions associated with the Boolean Operator are deleted.

Note: See the condition expression displayed under Filter string to see the logic of the expression as it is modified.

[Click here](#) for more information about using the Boolean Operators.

- Add your highest level Boolean operator first.
- The AND and OR Boolean Operators must contain at least two conditions.
- Add each additional Boolean Operator before adding the condition to which it applies.
- Place the cursor on the Boolean Operator that you want to append to or replace.

To edit a condition: Use the [rule components](#) to [insert](#)⁴, [append](#)⁵, and [replace](#)⁶ a condition.

Component	Description
Attribute	The attribute on which you want NNM iSPI Performance for QA to filter the probes. The listed attributes depend on the type of the QA Group selected.
Operator	The operator that establishes the relationship between the Attribute and Value.
Value	The value that completes the criteria required to define the condition.

Note: It is recommended to group the QA probes with millisecond precision value and microsecond precision value into separate QA groups.

4. Click  **Save** or  **Save and close**.

¹Adds the current Boolean Operator to the beginning of the selected Boolean Operator within the Filter String.

²Adds the current Boolean Operator to the end of the selected Boolean Operator within the Filter String.


³Replaces the selected Boolean Operator with the current Boolean Operator within the Filter String.

⁴Adds the current condition (Attribute, Operator, and Value) to the beginning of the conditions already added to the selected boolean operator.

⁵Adds the current condition (Attribute, Operator, and Value) to the end of the conditions already added to the selected boolean operator.




⁶Replaces the selected condition with the current condition within the Filter String.

Note: Ensure you click the  **Save** or  **Save and Close** in the Edit QA Groups form, after you edit to save the changes you made.

5. Click  Refresh in the QA Groups panel.
6. Click **Apply Now**.

Deleting QA Groups

To delete an existing QA Group:

1. [Launch the QA Groups Configuration form](#).
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Sites/QA Groups** > **QA Group**. The QA Groups Configuration form opens.
2. Select the QA Group that you want to delete, and click  **Delete** in the **Configured QA Groups** tab.
or
Click  **Delete All** to delete all the QA Groups.
3. Click  Refresh in the Configured QA Groups tab to view the changes.

Alternatively, you can use the following command to delete the selected QA groups:

Linux: `$NmInstallDir/bin/nmsqacustomgrouputil.ovpl -u <username> -p <password> -delete -g <QA group name>`

Windows: `%NmInstallDir%\bin\nmsqacustomgrouputil.ovpl -u <username> -p <password> -delete -g <QA group name>`


If you delete a QA Group, the QA Group information is deleted from the QA Groups Inventory View. However, deleting a QA group does not delete the QA probes associated with the group.

Note: `-u <username> -p <password>` are optional parameters.

Exporting QA Group Configurations

To export the QA probes associated with a QA group to an XML file:

1. [Launch the QA Groups Configuration form](#).
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Sites/QA Groups** > **QA Group**. The QA Groups Configuration form opens.

2. Click  **Export**.
3. In the user prompt dialog box, enter the file name where you want to export the configurations for the existing QA groups.
You must enter the file name with full path information. For example, C:\temp\QAGroup_conf.xml
4. Click **OK**.

You can also export QA group configurations using the following command line utilities:

QA Group Command	Command Behavior
<code>nmsqacustomgrouputil.ovpl -u <username> -p <password> -export <filename to export the QA group configurations></code>	Exports the QA group configurations to the specified XML file. Provide absolute path for the file where you want to export the QA group configurations.

If the QA group export fails, check the following log files:

Linux: \$NnmDataDir/log/qa/qa.log


Windows: %NnmDataDir%\log\qa\qa.log

Note: You can export QA group configurations for local and remote QA groups.

Note: -u <username> -p <password> are optional parameters.

Importing QA Group Configurations

To import QA group configurations from an XML file:

1. [Launch the QA Groups Configuration form](#).
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Sites/QA Groups** > **QA Group**. The QA Groups Configuration form opens.
2. Click  **Import**.
3. In the user prompt dialog box, enter the file name from where you want to import the QA group configuration information.
You must enter the file name with full path information. For example, C:\temp\QAGroup_conf.xml
4. Click **OK**.
If a QA group is already defined and displayed in the Configured QA group panel, the import utility does not import the configuration information for that group from the XML file.

You can also import QA group configuration information using the following command line utility:

Linux: \$NnmInstallDir/bin/nmsqacustomgrouputil.ovpl -u <username> -p <password> -import <filename to import the QA group configurations>

Windows: %NnmInstallDir%\bin\nmsqacustomgrouputil.ovpl -u <username> -p <password> -import - <filename to import the QA group configurations>

If the QA group import fails, check the following log files:

Linux: \$NnmDataDir/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Note: -u <username> -p <password> are optional parameters.

Operators Used in Defining QA Group Filter

The various operators that are used with the attributes in defining the QA Group filters are given below:

Operator	Description						
=	Finds all values equal to the value specified. For example, Node Group = Cisco finds all the node groups with the name Cisco .						
!=	Finds all values not equal to the value specified. For example, Node Group != Cisco finds all the node groups other than Cisco .						
like	Finds matches using wild card characters. For example, Interface Description (ifDescr) like Fa 0/1 finds all interface names that begin with Fa 0/1 .						
Not like	Finds all that do not have the values specified (using wild card strings). For example, Interface Description (ifDescr) not like Fa 0/1 finds all interface names that do not begin with Fa 0/1 .						
In	<p>Finds a match to at least one of the values specified. For example:</p> <table border="1"> <thead> <tr> <th>Attribute</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Policy Name</td> <td>P1</td> </tr> <tr> <td></td> <td>P2</td> </tr> </tbody> </table> <p>Finds all policy names that are P1 or P2.</p> <p>Note: You must enter each value in a separate line.</p>	Attribute	Value	Policy Name	P1		P2
Attribute	Value						
Policy Name	P1						
	P2						
Not in	<p>Finds all values except those included in the list of values. For example:</p> <table border="1"> <thead> <tr> <th>Attribute</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Policy Name</td> <td>P1</td> </tr> <tr> <td></td> <td>P2</td> </tr> </tbody> </table> <p>finds all policy names other than P1 and P2.</p>	Attribute	Value	Policy Name	P1		P2
Attribute	Value						
Policy Name	P1						
	P2						

Operator	Description
	Note: You must enter each value in a separate line.
Between	Finds all values equal to and between the two values specified. Use this operator only on attributes that have numeric values.
Not between	Finds all values except those between the two values specified. Use this operator only on attributes that have numeric values.
Range	Finds all values within the specified IP address range. You can specify the range in one of the following formats: <ul style="list-style-type: none"> • Wild card characters in place of octets For example: <ul style="list-style-type: none"> • 192.168.*.* • Ranges of numbers in place of octets For example: <ul style="list-style-type: none"> • 192.168.10-20.2 • 192.168.10-25.5-25 • Subnet address For example, 192.168.0.0/8
<	Finds all values less than the value specified. For example, Target address < 192.168.215.215 finds all the IP addresses less than 192.168.215.215
<=	Finds all values less than or equal to the value specified. For example, Target address <= 192.168.215.215 finds all the IP addresses less or equal to 192.168.215.215
>	Finds all values greater than the value specified. For example, Target address > 192.168.215.215 finds all the IP addresses greater than 192.168.215.215
>=	Finds all values greater than or equal to the value specified. For example, Target address >= 192.168.215.215 finds all the IP address greater than or equal to 192.168.215.215

Values Used in Defining QA Group Filter

A list of values is available for some of the attributes when defining a QA group filter. The following table lists those attributes and the values you can choose for them:

Group Type	Attribute	Value
QA Probes	Probe Type	ICMP Echo UDP Echo

Group Type	Attribute	Value
		UDP TCP connect VOIP HTTP HTTPS Oracle DNS DHCP ICMP Jitter
CBQoS	Action Type	Queuing RED Shaping Policing Packet Marking
	Policy Direction	Ingress Egress Both Not Applied

Chapter 7: Configuring Thresholds

Using thresholds, NNM iSPI Performance for QA enables you to track the health and performance of the [network elements](#)¹ in a network.

You can establish thresholds for the network elements monitored by NNM iSPI Performance for QA and configure these thresholds to create incidents whenever the network performance measurement assigned breaches the threshold.

For information about configuring thresholds, see the following topics:

- ["Configuring Probe Thresholds" on the next page](#)
- ["Configuring Probe Thresholds for QA Groups" on page 234](#)
- ["Configuring Site Thresholds" on page 251](#)
- ["Configuring QoS Thresholds" on page 270](#)
- ["Configuring QoS Thresholds for QA Groups" on page 284](#)
- ["Configuring Ping Latency Pair Thresholds" on page 293](#)

¹Some examples of network elements are routers and switches.

Configuring Probe Thresholds

You can use the Configure Threshold form to perform the following tasks:

- Configure the threshold values for the metrics of selective QA probes
- Override the threshold values for the metrics of selective QA probes, which may or may not be associated with a site

You can configure thresholds for the following metrics assigned to the QA probes:

- Round Trip Time (RTT)
- Jitter
- Packet Loss (Can be from source to destination, and from destination to source.)
- [Mean Opinion Score \(MOS\)](#)

NNM iSPI Performance for QA performs the following actions if a threshold is breached:

- Sets the QA probe status to Major.
- Creates an incident for the violated threshold.
- Sends the threshold violation details to the Network Performance Server for generating reports.
- Retains the threshold state as Nominal, or sets the threshold state to High or Low depending on the count-based, and time-based threshold configuration.

You cannot configure thresholds for [Remote QA Probes](#)¹.

You can monitor the network performance and generate an incident based on the count-based threshold configuration or time-based threshold configuration.

You can only configure either a count-based or time-based threshold configuration for a combination of a probe, service, and metric.

Threshold Configuration

Count-Based Threshold Configuration

You can generate an incident based on the count or number of consecutive times a metric violates the threshold value. You can define this count in the Threshold Configuration form.

Time-Based Threshold Configuration

Time-Based threshold configuration enables you to raise an alert when the threshold breached state persists for more than a specific time period. This is derived by specifying X as the duration of time in minutes when the metric is in a threshold breached state within Y number of minutes specified in the sliding window.

Example for Time-Based Threshold Configuration

¹At Global server, the probes discovered and forwarded by regional servers are called as remote probes. You can manage threshold for these probes only at regional manager.

Consider a scenario, where the polling interval is 5 minutes; High duration is 10 minutes; and High Duration Window is 60 minutes. In this scenario, an incident is generated whenever the High Duration exceeds 10 minutes within the 60 minute duration. NNM iSPI Performance for QA uses a sliding window wherein each time the High Duration (10 minutes) is reached, NNM iSPI Performance for QA drops the oldest polled value (first 5 minutes) and adds the most recent (between 60 to 65 minutes). This procedure continues and enables you to determine time-based threshold violation.

You can make utmost use of the Time-Based threshold violation by ensuring that the duration specified in the sliding window is greater than or equal to the polling interval.

Baseline Settings Configuration

Baseline Deviation Settings Configuration

Apart from the time-based and count-based threshold configuration, you can also do "Baseline Monitoring" based on the baseline deviation setting configuration in NNM iSPI Performance for QA. You can do baseline deviation setting configuration for the selected probe, service, and metric. An incident is generated and the baseline state transitions to Abnormal Range only if it meets all the criteria listed below:





- Exceeds the count or the number of [standard deviation](#) that is above the average value for the metric, or exceeds the count or the number of [standard deviation](#) that is below the average value for the metric. This count is specified in the Upper Baseline Limit Deviations or the Lower Baseline Limit Deviations in the baseline deviation settings configuration
- Exceeds the duration for which the upper or lower baseline deviation persists in the specified sliding window duration




Baseline Monitoring

Apart from the time-based and count-based threshold configuration, you can also do a baseline monitoring. Baseline monitoring is dynamic and updates the [baseline state](#) by comparing the extent of deviation from the average real-time data of the metric with the previous average values in a similar situation. For example, in a site during the peak hours or on week days, the RTT value is expected to exceed the high value frequently. In such a scenario, an incident need not be generated in the NNMi console. So, HP NNM iSPI Performance for Metrics Software enables you to compare the current threshold values during the peak hours with the previous set of values during the same peak hours. Based on the extent of deviation, you can configure to generate an incident in the NNMi console.

Baseline State

Baseline Monitoring sets a new state referred to as Baseline state for the QA probes. The valid baseline states for the QA probes are listed below:

-  Normal Range - The metric is within the normal range of deviation
-  Abnormal Range - The metric is either above or below the configured normal range of the deviation
-  Unavailable -The computed value for the metric is not found in HP NNM iSPI Performance for Metrics Software
-  Unset - No baseline is computed

-  Not polled - The metric is not polled for baseline deviations
-  No Polling Policy - No polling policy exists for this metric
-  Threshold Agent Error - Indicates an error was returned while retrieving the data from NPS by the state poller

Incidents

The following incidents are generated whenever there is a deviation from the configured normal range of deviation for the metric:

- RoundTripTimeAbnormal
- TwoWayPacketLossAbnormal
- TwoWayJitterAbnormal
- MeanOpinionScoreAbnormal

For more information about incidents, see ["Incidents " on page 28](#)



Launching the Configure Threshold Form

To launch the Configure threshold form:






1. Log on to NNMi console using your user name and password.
You must have administrator privileges.
2. From the workspace navigation panel, select **Quality Assurance**.
The Quality Assurance tab expands.
3. Select any one of the following inventory views:
 - QA Probes
 - Critical Probes
 - Threshold Exception Probes
 - Baseline Exception Probes
4. Select the QA probes for which you need to configure the threshold value.
You can select a maximum of 10 QA probes at a time.
5. Click **Actions** → **Quality Assurance** → **Configure Threshold**.
 - If you are configuring a new threshold value for the selected QA probes, the Add Threshold Configuration form opens.
 - If a threshold value already exists for the selected QA probes, the Edit Threshold Configuration form opens.

- If you selected [Remote QA Probes](#)¹, a message appears to indicate that you cannot configure thresholds for the remote QA probes. It also shows the list of remote QA probes selected.






6. You can do the following in the **Threshold Configuration Toolbar**:

Icon	Description
 Close	Closes the Threshold Configuration form without saving the current configuration.
 Save and Close	Saves the current configuration and closes the Threshold Configuration form.

7. You can do the following in the **Threshold Settings Tab**:

Icon	Description
 New	Adds threshold settings for the QA probes.
 Edit	Edits threshold settings for the QA probes.
 Delete	Deletes thresholds of the QA probes.
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data.
 Delete All	Deletes all the thresholds of the QA probes.


8. You can do the following in the **Baseline Settings Tab**:

Icon	Description
 New	Adds baseline settings for the QA probes.
 Edit	Edits baseline settings for the QA probes.
 Delete	Deletes the selected baseline setting of the QA probes.
 Refresh	Retrieves the last saved baseline settings configuration from the database and displays the data.
 Delete All	Deletes all the baseline settings of the QA probes.

¹At Global server, the probes discovered and forwarded by regional servers are called as remote probes. You can manage threshold for these probes only at regional manager.

Adding Threshold Settings

To add a new threshold setting:

1. Make sure that you selected the Source Site, and Service when [Adding Threshold Configuration](#).
2. Click  **New** in the **Threshold Settings** tab.
 The Add Threshold Settings form opens.
3. Specify the following to configure the threshold settings:



Field Name	Description
Type	Select the type of threshold violation. The valid types are Count-Based and Time-Based .
Metric	Select the metric for which you are configuring the threshold. The metrics are populated based on the service. For information about the metrics for each service type, see " Supported Threshold Configuration Metrics " on page 299.

4. After you select the metric to configure the threshold, the list of fields relevant to the selected metric appear. You can specify the following values to configure the new threshold:

Field Name	Description
High Value	Enter the threshold value. This value indicates the maximum value above which the metric will be considered to have violated the Nominal range. For Packet Loss metric, enter the High Value in percentage.
High Value Rearm	<p>Enter the high value rearm for the threshold. For Packet Loss metric, enter the High Value Rearm in percentage.</p> <p>The High Value Rearm is used to indicate the end of the high threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value.</p> <p>The high value rearm must always be lower than the high value.</p> <p>Example</p> <p>For the Round Trip Time (RTT) you must generate an incident when the RTT is 150 and clear the incident when the RTT value comes down to 100.</p> <p>Set the following values for the threshold:</p> <ul style="list-style-type: none"> • High Value: 150 • High Value Rearm: 100 <p>This value enables you to be aware when a network</p>

Field Name	Description
	performance problem starts to improve.
Low Value	Enter the low threshold value. This value indicates the minimum value below which the metric will be considered to have violated the Nominal range.
Low Value Rearm	<p>Enter the low value rearm for the threshold. For Packet Loss metric, enter the Low Rearm Value in percentage.</p> <p>The low value rearm is used to indicate the end of the low threshold state and NNM iSPI Performance for QA clears the incident once it reaches above this value.</p> <p>The low value rearm must be greater than the low value.</p> <p>Example</p> <p>For the Mean Opinion Score (MOS) you must generate an incident when the MOS score is 3 and clear the incident when the score is improved to 4.5.</p> <p>Set the following values for the threshold:</p> <ul style="list-style-type: none"> • Low Value: 3 • Low Value Rearm: 4.5 <p>This value enables you to be aware when a network performance problem starts to improve.</p>

The following field appears, if you selected the Type as Count-Based:

Field Name	Description
Trigger Count	Specify after how many consecutive threshold violations NNM iSPI Performance for QA must alert the operator by transitioning the threshold state to  High or  Low accordingly.

The following fields appear if you selected the Type as Time-Based:

Field Name	Description
High Duration	<p>Designate the minimum time within which the metric value must remain in the High range.</p> <p>For example if you specify this value to be 20 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 minutes.</p> <p>You define the high threshold value in the High Value field.</p> <p>The High Duration should be equal to or greater than the associated Polling Interval setting, because that is how often</p>

Field Name	Description
	NNM iSPI Performance for QA provides a data point..
High Duration Window	<p>Designate the window of time within which the High Duration criteria must be met.</p> <p>To enable this setting, the value must be:</p> <ul style="list-style-type: none"> • greater than 0 (zero) • the same as or greater than the High Duration value <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p> <p>For example, if you specify this value to be 30 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 out of 30 minutes.</p>

The following fields appear if you selected the Type as Time-Based and the metric as MOS:



Low Duration	<p>Designate the minimum time within which the metric value must remain in the Low range.</p> <p>For example if you specify this value to be 20 minutes for MOS metric, NNM iSPI Performance for QA considers the threshold to be violated if the MOS is low for 20 minutes.</p> <p>You define the low threshold value in the Low Value field.</p> <p>The polling interval should be less than or equal to the Low Duration.</p>
Low Duration Window	<p>Designate the window of time within which the Low Duration criteria must be met.</p> <p>For example, if you specify this value to be 30 minutes for MOS metric, NNM iSPI Performance for QA considers the threshold to be violated if the MOS is low for 20 out of 30 minutes.</p> <p>To enable this setting, the value must be:</p> <ul style="list-style-type: none"> • greater than 0 (zero) • the same as or greater than the Low Duration value <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p>

5. Select the following to generate an incident when the time-based threshold or count-based

threshold value is violated:



Field Name	Description
Generate Incident	Select this option if you want NNM iSPI Performance for QA to generate an incident. By default this option is selected.

6. Use any one of the following options to complete the task:

Icons	Description
 Close	Closes the Add Threshold Configuration form without saving the threshold information you have entered.
 Save and Close	Saves the threshold information and closes the Threshold Configuration form

7. Click  **Refresh** to view the changes.

8. Click  **Save** or  **Save and Close** in the Threshold Configuration form.

Caution: The new threshold is not saved unless you click  **Save** or  **Save and Close** in the Threshold Configuration form.

NNM iSPI Performance for QA applies the following rules when creating thresholds for a **site** using this form:

- You can create thresholds only for the existing sites.
- You must select a source site and service for the new threshold.
- You could select the destination site for the new threshold
- If you do not specify a destination site for the threshold, the threshold is applied to all the destination sites of the source sites.
- You cannot configure thresholds for remote sites.


Time-Based Threshold cannot be configured for QA probes, if the polling interval is greater than the High Duration or Low Duration value. A list of these QA Probes, the UUID, and other details can be viewed in the log file, which is available in the following directory:

Linux: \$NnmDataDir/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Editing Threshold Settings

To edit an existing threshold setting:

1. Specify all the mandatory fields when [editing threshold configuration](#).
 - a. Select the metric, and click  **Edit** in the **Threshold Settings** tab.
The Edit Threshold Settings form opens.

Caution: You cannot edit the metric type and threshold type (Time-based or Count-based). If you want to edit the metric type or threshold type (Time-based or Count-based), delete the existing configuration settings and configure a new threshold settings, based on your requirements.

2. You can specify the following values to edit the threshold:



For probe based threshold configuration, you can view the threshold that was configured for the Remote QA probes, but you **cannot** configure thresholds for [Remote QA Probes](#)¹.

Field Name	Description
High Value	Enter the threshold value. This value indicates the maximum value above which the metric will be considered to have violated the Nominal range. For Packet Loss metric, enter the High Value in percentage.
High Value Rearm	<p>Enter the high value rearm for the threshold. For Packet Loss metric, enter the High Value Rearm in percentage.</p> <p>The High Value Rearm is used to indicate the end of the high threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value.</p> <p>The high value rearm must always be lower than the high value.</p> <p>Example</p> <p>For the Round Trip Time (RTT) you must generate an incident when the RTT is 150 and clear the incident when the RTT value comes down to 100.</p> <p>Set the following values for the threshold:</p> <ul style="list-style-type: none"> • High Value: 150 • High Value Rearm: 100 <p>This value enables you to be aware when a network performance problem starts to improve.</p>
Low Value	Enter the low threshold value. This value indicates the minimum value below which the metric will be considered to have violated the Nominal range.
Low Value Rearm	<p>Enter the low value rearm for the threshold. For Packet Loss metric, enter the Low Rearm Value in percentage.</p> <p>The low value rearm is used to indicate the end of the low threshold state and NNM iSPI Performance for QA clears the incident once it reaches above this value.</p>

¹At Global server, the probes discovered and forwarded by regional servers are called as remote probes. You can manage threshold for these probes only at regional manager.

Field Name	Description
	<p>The low value rearm must be greater than the low value.</p> <p>Example</p> <p>For the Mean Opinion Score (MOS) you must generate an incident when the MOS score is 3 and clear the incident when the score is improved to 4.5.</p> <p>Set the following values for the threshold:</p> <ul style="list-style-type: none"> • Low Value: 3 • Low Value Rearm: 4.5 <p>This value enables you to be aware when a network performance problem starts to improve.</p>

The following fields appear, if the Type is Count-Based, and you can modify the information if required

Field Name	Description
Trigger Count	Specify after how many consecutive threshold violations NNM iSPI Performance for QA must alert the operator by transitioning the threshold state to  High or  Low accordingly.

The following fields appear if the Type is Time-Based, and you can modify the information if required:

Field Name	Description
High Duration	<p>Designate the minimum time within which the metric value must remain in the High range.</p> <p>For example if you specify this value to be 20 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 minutes.</p> <p>You define the high threshold value in the High Value field.</p> <p>The High Duration should be equal to or greater than the associated Polling Interval setting, because that is how often NNM iSPI Performance for QA provides a data point..</p>
High Duration Window	<p>Designate the window of time within which the High Duration criteria must be met.</p> <p>To enable this setting, the value must be:</p> <ul style="list-style-type: none"> • greater than 0 (zero) • the same as or greater than the High Duration value

Field Name	Description
	<p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p> <p>For example, if you specify this value to be 30 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 out of 30 minutes.</p>

The following fields appear, if you selected the Type as Time-Based and the metric as MOS:



You can modify the information if required.




Low Duration	<p>Designate the minimum time within which the metric value must remain in the Low range.</p> <p>For example if you specify this value to be 20 minutes for MOS metric, NNM iSPI Performance for QA considers the threshold to be violated if the MOS is low for 20 minutes.</p> <p>You define the low threshold value in the Low Value field.</p> <p>The polling interval should be less than or equal to the Low Duration.</p>
Low Duration Window	<p>Designate the window of time within which the Low Duration criteria must be met.</p> <p>For example, if you specify this value to be 30 minutes for MOS metric, NNM iSPI Performance for QA considers the threshold to be violated if the MOS is low for 20 out of 30 minutes.</p> <p>To enable this setting, the value must be:</p> <ul style="list-style-type: none"> greater than 0 (zero) the same as or greater than the Low Duration value <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p>



- Select the following to generate an incident when the time-based threshold or count-based threshold value is violated:

Field Name	Description
Generate Incident	Select this option if you want NNM iSPI Performance for QA to generate an incident for count-based or time-based threshold violations. By default this option is selected.

4. Use any one of the following options to complete the task:

Icons	Description
 Close	Closes the Add Threshold Configuration form without saving the threshold information you have entered
 Save and Close	Saves the threshold information and closes the Threshold Configuration form

5. Click  **Refresh** in the Threshold Settings panel to view the changes.
6. Click  **Save** or  **Save and Close** in the Threshold Configuration form.

Note: The changes you have made in the threshold is not saved unless you click  **Save** or  **Save and Close** in the Threshold Configuration form.


NNM iSPI Performance for QA applies the following rules while updating thresholds:

- You can define thresholds only for the existing sites.
- Any modification in the threshold directly updates the state poller.

Time-Based Threshold cannot be configured for QA probes, if the polling interval is greater than the High Duration or Low Duration value. A list of these QA Probes, the UUID, and other details can be viewed in the log file, which is available in the following directory:


Linux: \$NnmDataDir/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Note: You can select all the threshold configured settings and click  **Edit** option, but edit form will open for only one threshold group.

Adding Baseline Settings

To add a new baseline setting configuration:

1. Make sure that you selected the Source Site, and Service in the [adding threshold configuration](#) .
2. Click  **New** in the **Baseline Settings** tab.
The Add Baseline Settings form opens.
3. Specify the following to configure the baseline deviation settings:

Field Name	Description
Metric	Select the metric for which you require to configure baseline deviation settings. The valid metrics for baseline deviation setting configuration are as below: <ul style="list-style-type: none"> • RTT (ms)



Field Name	Description
	<ul style="list-style-type: none"> • RTT (microS) • Two Way Jitter (microS) • Two Way Packet Loss (%) • MOS




4. After you select the metric, the list of fields relevant to the selected metric appear. You can specify the following values to configure the baseline deviation settings:



Field Name	Description
Upper Baseline Limit Enabled	<p>If enabled, NNM iSPI Performance for QA uses the Upper Baseline Limit attribute value to determine the number of standard deviations above the average that defines the upper baseline limit.</p> <p>If disabled, NNM iSPI Performance for QA does not define the upper baseline limit.</p> <p>This field is not applicable to MOS metric.</p>
Upper Baseline Limit Deviations - Above Average	<p>Enter the number of standard deviation s above the average values that NNM iSPI Performance for QA should use to determine the upper baseline limit.</p> <p>This field is not applicable to MOS metric.</p>
Lower Baseline Limit Enabled	<p>If enabled, NNM iSPI Performance for QA uses the Lower Baseline Limit attribute value to determine the number of standard deviations below the average that defines the lower baseline limit.</p> <p>If disabled, NNM iSPI Performance for QA does not define the lower baseline limit.</p> <p>This field is applicable to MOS metric only.</p>
Lower Baseline Limit Deviations - Below Average	<p>Enter the number of standard deviation below the average values that NNM iSPI Performance for QA should use to determine the lower baseline limit.</p> <p>This field is applicable to MOS metric only.</p>
Duration	<p>The minimum time for which the standard deviation must persist to deviate from the configured Baseline Range before the baseline state transitions to Abnormal Range and generates an incident.</p> <p>The Polling Interval should be less than or equal to the Duration.</p>

Field Name	Description
Window Duration	<p>The window duration within which the Upper Baseline Limit or Lower Baseline Limit Deviation criteria must be met.</p> <p>The value must be greater than 0 (zero) and can be the same as the Duration value.</p> <p>The NNM iSPI Performance for QAs uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p>

5. Use any one of the following options to complete the task:

Icon	Description
 Close	Closes the Add Baseline Settings form without saving the baseline setting information you have entered.
 Save and Close	Saves the baseline setting information and closes the Add Baseline Settings form.

6. Click  **Save and Close** in the Add Baseline Settings form to save the baseline setting information.
7. Click  **Save** or  **Save and Close** in the Threshold Configuration form.

The new baseline settings configuration is not saved unless you click  **Save** or  **Save and Close** in the Threshold Configuration form.

NNM iSPI Performance for QA applies the following rules while configuring baseline deviation settings for a **site** using this form:

- You can configure baseline settings only for the QA probes of the existing sites.
- You must select a source site, service, and metric to configure the baseline settings.
- Optionally, you can select the destination site
- If you do not specify a destination site for the baseline setting, the configuration is applied to all the QA probes of the destination sites from the source sites.
- You cannot configure baseline settings for remote sites.

Editing Baseline Settings

To edit a baseline setting configuration:

1. Make sure that you selected the Source Site, and Service when [editing threshold configuration](#) if you are launching the form from Site Wide threshold configuration. You can ignore this step if you are launching this form from Probe-based threshold configuration.

2. Select the baseline settings, and click  **Edit** in the **Baseline Settings** panel.

The Edit Baseline Settings form opens.

3. In the **Baseline Deviations Settings** panel:

- a. You can view the following details:

Field Name	Description
Metric	The metric for which you require to edit the baseline deviations settings configuration.



- b. You can edit the following baseline deviation settings configuration:


The following fields appear depending on the metric:



Field Name	Description
Upper Baseline Limit Enabled	If enabled, NNM iSPI Performance for QA uses the Upper Baseline Limit attribute value to determine the number of standard deviations above the average that defines the upper baseline limit. If disabled, NNM iSPI Performance for QA does not define the upper baseline limit. This field is not applicable to MOS metric.
Upper Baseline Limit Deviations - Above Average	Enter the number of standard deviation s above the average values that NNM iSPI Performance for QA should use to determine the upper baseline limit. This field is not applicable to MOS metric.
Lower Baseline Limit Enabled	If enabled, NNM iSPI Performance for QA uses the Lower Baseline Limit attribute value to determine the number of standard deviations below the average that defines the lower baseline limit. If disabled, NNM iSPI Performance for QA does not define the lower baseline limit. This field is applicable to MOS metric only.
Lower Baseline Limit Deviations - Below Average	Enter the number of standard deviation below the average values that NNM iSPI Performance for QA should use to determine the lower baseline limit. This field is applicable to MOS metric only.
Duration	The minimum time for which the standard deviation must persist to deviate from the configured Baseline Range before the baseline state transitions to Abnormal Range and generates an incident. The Polling Interval should be less than or equal to the Duration.



Field Name	Description
Window Duration	<p>The window duration within which the Upper Baseline Limit or Lower Baseline Limit Deviation criteria must be met.</p> <p>The value must be greater than 0 (zero) and can be the same as the Duration value.</p> <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p>

4. Use any one of the following options to complete the task:

Icon	Description
 Close	Closes the Edit Baseline Settings form without saving the baseline setting information you have entered.
 Save and Close	Saves the baseline setting information and closes the Edit Baseline Settings form

5. Click  **Save and Close** in the Edit Baseline Settings form to save the baseline setting information.

6. Click  **Save** or  **Save and Close** in the Site Wide Threshold Configuration form.


The new baseline settings configuration is not be saved unless you click  **Save** or  **Save and Close** in the Threshold Configuration form.


NNM iSPI Performance for QA applies the following rules while configuring baseline deviation settings for a **site** using this form:

- You can configure baseline settings only for the QA probes of the existing sites.
- You must select a source site and service to configure the baseline settings.
- Optionally, you could select the destination site.
- If you do not specify a destination site for the baseline setting, the configuration is applied to all the QA probes of the destination sites from the source sites.
- You cannot configure baseline settings for remote sites.

Deleting Thresholds


To delete an existing threshold of QA probes:

1. [Launch the Configure Threshold form](#) .
2. Select a threshold in the **Threshold Settings** panel and click  **Delete**.
or

Click  **Delete All** to delete all thresholds of QA probes.

3. Click  **Refresh** in the Threshold Settings panel to view the changes.

The following changes occur after deleting a probe based threshold configuration:

The selected thresholds configured for the metrics of the QA probe are deleted and the threshold state is set to  **Threshold Not Set** for the metric. The QA Probe status is set to the most severe status. If the QA probe is associated with a site, the threshold state configured for the metric in the site is associated with the QA probe. The incidents and conclusions are updated accordingly.

Example 1

Consider the following scenario:

Before Deleting the Threshold(s) Configured for the QA Probe:

QA Probe Status :  Major

Threshold State:  High

Note: The threshold state is high for RTT and Packet Loss

Conclusion: RttThresholdStateHigh, TwoWayPktLossThresholdStateHigh, RTTAbnormal

After Deleting the Threshold(s) Configured for the QA Probe:

QA Probe Status :  Major

Threshold State:  Threshold Not Set

Note: The threshold state is set to Threshold Not Set for RTT and Packet Loss. If the QA probe is associated with a site the Threshold State is updated based on the threshold configured for the site.

Conclusion: RTTAbnormal

The QA Probe Status is still set to Major as the Baseline State is in the Abnormal Range.

Example 2

Consider the following scenario:

Before Deleting the Threshold(s) Configured for the QA Probe:

QA Probe Status :  Major

Threshold State:  High

Conclusion: TestUp¹, RttThresholdStateHigh, TwoWayPktLossThresholdStateHigh

After Deleting the Threshold(s) Configured for the QA Probe:

QA Probe Status :  Normal

Threshold State:  Threshold Not Set

¹When both Administrative and Operational states are up.

If the QA probe is associated with a site the Threshold State is updated based on the threshold configured for the site.

Conclusion: [TestUp](#)¹

Troubleshooting Threshold Configuration Error Messages

The error log files are available in the following directory:

Linux: `./var/opt/OV/log/qa/qa.log`

Windows: `%NnmDataDir%\log\qa\qa.log`

[Selected different service type. Deleting all settings.](#)


Occurs when you select a different service type, while creating a new threshold or editing an existing threshold.

Reason and Resolution

NNM iSPI Performance for QA creates threshold for a metric based on the service type you have selected. Metrics available for different service types are different. For example, if you select TCP Connect service type, you can set thresholds for only the [Round Trip Time \(RTT\)](#) metric.



Changing the service type for a threshold may need you to update the threshold values for all the metrics. NNM iSPI Performance for QA deletes all the metric threshold values you have set previously, if you select a different service type.

[Configuration already has the possible settings. Cannot add more.](#)

Occurs if you click  **New** in the Threshold Settings panel of the Add Threshold Configuration form after creating a threshold.

Reason and Resolution

While creating a threshold, you performed the following steps:

1. Selected the following values in the Threshold Configuration panel in the Add Threshold Configuration form:
 - a. Source Site
 - b. Destination Site
 - c. Service Type
2. Clicked  **New** in the Add Threshold Settings panel.
3. In the Threshold Configuration form, you selected the metric, high value, low value, high value rearm, low value rearm, etc.
4. Selected  **Save and Close** in the Threshold Configuration form. The threshold is added in the Threshold Settings panel of the Add Threshold Configuration form.

¹When both Administrative and Operational states are up.

5. Clicked **New** in the Threshold Settings panel.
6. The system displays an error message saying "The threshold already has the possible settings. Cannot add more."

You cannot add more than one set of threshold settings for a threshold configuration.

Failed to import the threshold configuration. Please check the log files.

Occurs under any of the following circumstances:

- If the import file does not exist in the path you entered.
- If a threshold is already defined and displayed in the Site Wide Threshold Settings panel.

Reason and Resolution

NNM iSPI Performance for QA imports the threshold configuration from an XML file. If the file path is not correct, NNM iSPI Performance for QA fails to import the configuration information.

Also the import utility does not import the threshold configuration if the configuration is unchanged since the last import

Check any of the following log files:

Linux: ./var/opt/OV/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Failed to export the threshold configuration. Please check the log files.

Occurs under any of the following circumstances:

- If the export file path that you entered is incorrect.
- If the threshold is not associated with at least one site.

Reason and Resolution

NNM iSPI Performance for QA exports the threshold configuration to an XML file. If the file path is not correct, NNM iSPI Performance for QA fails to export the configuration information.

To define a threshold configuration you must associate it with at least one source site. You may or may not associate the threshold to a destination site.

Check any of the following log files:

Linux: ./var/opt/OV/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Duration of poll window cannot be greater than duration of sliding window

Occurs when the duration of the sliding window or Window Duration is greater than the polling window.

Reason and Resolution

The polling window duration must be lesser than the sliding window duration

Duration should be between 0 and 1400 minutes(1 day)

Occurs when the low duration or high duration value (in minutes) for a time-based threshold is not within the range

Reason and Resolution

The Low Duration or the High Duration value(in minutes) for a time-based threshold must be within the range 0 to 1400 minutes (equivalent to 1 day).

Duration should be between 0 and 60 seconds

Occurs when the low duration or high duration value (in seconds) is not within the range

Reason and Resolution

The Low Duration or the High Duration value(in seconds) must be within the range 0 to 60 seconds

Import failed, file not found

Occurs when you import a threshold configuration

Reason and Resolution

You must import by specifying the absolute path of the file, and you must check the XML filename as well. The file to be imported must be available on the NNMi management server.

Viewing Probe-Specific Thresholds


To launch the probe specific threshold configuration form:

1. Log on to NNMi console using your user name and password.
You must have administrator privileges.
2. From the workspace navigation panel, select **Configuration** workspace.
3. Select **Quality Assurance Configuration Console**.
The console opens.
4. In the **Configuration** workspace, select **Threshold Configuration > Probes >Probe Specific Threshold**.
The Probe Specific Threshold form opens.
For more information about configuring probe thresholds, see "[Configuring Probe Thresholds](#)" on page 213.
A list of all the probes for which thresholds are already configured appears. You can view the following for each of the discovered probes:




Probes with Specific Thresholds

Attribute Name	Description
Name	The name of the QA probe configured in the network device.
Service	The type of the QA probe. Some of the QA probe types that the NNM iSPI Performance for QA recognizes are as follows: <ul style="list-style-type: none"> • UDP Echo • ICMP Echo • UDP Echo • TCP Connect • VoIP
Owner	The name of the QA probe's owner.
Source	The source device from which the probe is configured.
Destination	The destination network device to which the probe is configured.
ToS	Type of Service specified in an IP packet header that indicates the service level required for the packet.
Settings Preview	Move the mouse over this icon to view a snapshot of all the threshold settings configured for the probe.

5. You can perform the following tasks using the Probe Specific Threshold Toolbar:

Icon	Description
 Close	Closes the Threshold Configuration form without saving the current configuration.

6. You can perform the following tasks using the Probes With Specific Thresholds Tab:

Icon	Description
 Edit Configured Settings	Edits the selected probe based threshold configuration.
 Delete Configured Settings	Deletes an existing probe based threshold configuration.
 Refresh	Retrieves the last saved data from the database and displays the data in the view

Configuring Probe Thresholds for QA Groups

NNM iSPI Performance for QA enables you to track the health and performance of the QA groups, which you have configured and discovered. You can configure thresholds for QA groups and create incidents whenever the performance value assigned to the QA groups breaches the threshold.

Note: For configuring thresholds for probes, it is recommended to use the QA group-based threshold configuration than the site-based threshold configuration. For more information about configuring thresholds for QA groups, see ["Adding QA Group Threshold Configuration" on the next page](#)

NNM iSPI Performance for QA performs the following actions, if a threshold is breached:

- Sets the QA Groups probes' status to major.
- Creates an incident for the violated threshold.
- Retains the threshold state as Nominal, or sets the threshold state to High or Low depending on the count-based, or time-based threshold configuration.

You can monitor the QA Groups entities and generate an incident based on the count-based threshold configuration or time-based threshold configuration.

Threshold Configuration

Count-Based Threshold Configuration

You can generate an incident based on the count or number of consecutive times a metric violates the threshold value. You can define this count in the Threshold Configuration form.

Time-Based Threshold Configuration

Time-Based threshold configuration enables you to raise an alert when the threshold breached state persists for more than a specific time period. This is derived by specifying X as the duration of time in minutes when the metric is in a threshold breached state within Y number of minutes specified in the sliding window.

Example for Time-Based Threshold Configuration

Consider a scenario, where the polling interval is 5 minutes; High duration is 10 minutes; and High Duration Window is 60 minutes. In this scenario, an incident is generated whenever the High Duration exceeds 10 minutes within the 60 minute duration. NNM iSPI Performance for QA uses a sliding window wherein each time the High Duration (10 minutes) is reached, NNM iSPI Performance for QA drops the oldest polled value (first 5 minutes) and adds the most recent (between 60 to 65 minutes). This procedure continues and enables you to determine time-based threshold violation.

You can make utmost use of the Time-Based threshold violation by ensuring that the duration specified in the sliding window is greater than or equal to the polling interval.

Baseline Settings Configuration

Baseline Deviation Settings Configuration


Apart from the time-based and count-based threshold configuration, you can also do **baseline monitoring** based on the baseline deviation setting configuration in NNM iSPI Performance for QA. You can do baseline deviation setting configuration for the selected probe, service, and metric. An incident is generated and the baseline state transitions to Abnormal Range only if it meets all the criteria listed below:

- Exceeds the count or the number of standard deviation that is above the average value for the metric, or exceeds the count or the number of standard deviation that is below the average value for the metric. This count is specified in the Upper Baseline Limit Deviations or the Lower Baseline Limit Deviations in the baseline deviation settings configuration
- Exceeds the duration for which the upper or lower baseline deviation persists in the specified sliding window duration

Note: HP recommends that you have the probes with same frequency in a QA group for the Baseline Threshold feature to work effectively.

Adding QA Group Threshold Configuration

To add a new QA Group threshold:






1. [Launch the Threshold Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Threshold Configuration** > **Probes** > **Sites/QA Group**. The Threshold Configuration form opens.
2. Click  **New** in the Threshold Configuration form panel. The threshold configuration form opens.
3. Specify the following to configure the threshold:

Field Name	Description
Threshold Type	In the Threshold Type, select QA Groups Based .
Order	Specify a numeric value. NNM iSPI Performance for QA checks the configuration settings in the order you define (lowest number first).
QA Group	Lists the configured and discovered QA Probes that belong to the QA Group. You can select any one of the configured and discovered QA Groups, from the drop down list to configure the threshold.
Service	The type of the discovered QA probe. This field is mandatory. NNM iSPI Performance for QA recognizes the following QA probe types: <ul style="list-style-type: none">• UDP Echo• ICMP Echo• UDP






Field Name	Description
	<ul style="list-style-type: none"> • TCP Connect • VoIP • HTTP • DNS

You can view the two tabs; Threshold Settings and Baseline Settings.

4. You can perform the following tasks when you click on the **Threshold Settings** tab:

Icons	Description
 New	Creates QA Group thresholds.
 Edit	Edits QA Group thresholds.
 Delete	Deletes QA Group thresholds.
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data.
 Delete All	Deletes all QA Group thresholds.

5. You can perform the following tasks when you click on the **Baseline Settings** tab:

Icons	Description
 New	Creates QA Group baseline threshold settings.
 Edit	Edits QA Group baseline threshold settings.
 Delete	Deletes QA Group baseline threshold settings.
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data.
 Delete All	Deletes all QA Group baseline threshold settings.

Adding QA Group for QA Probe Threshold Setting

To add a new threshold:

1. Specify all the mandatory fields when [adding QA groups threshold settings.](#)
2. Click

*** New in the Threshold Settings tab.**

The Add Threshold Settings form opens.

- Specify the following to configure the threshold settings:



Field Name	Description
Type	Select the type of threshold violation. The valid types are Count-Based and Time-Based .
Metric	Select the metric for which you are configuring the threshold. The metrics are populated based on the service. For information about the metrics for each service type, see "Supported Threshold Configuration Metrics" on page 299 .

- After you select the metric to configure the threshold, the list of fields relevant to the selected metric appear. You can specify the following values to configure the new threshold:

Field Name	Description
High Value	Enter the threshold value. This value indicates the maximum value above which the metric will be considered to have violated the Nominal range. For Packet Loss metric, enter the High Value in percentage.
High Value Rearm	<p>Enter the high value rearm for the threshold. For Packet Loss metric, enter the High Value Rearm in percentage.</p> <p>The High Value Rearm is used to indicate the end of the high threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value.</p> <p>The high value rearm must always be lower than the high value.</p> <p>Example</p> <p>For the Round Trip Time (RTT) you must generate an incident when the RTT is 150 and clear the incident when the RTT value comes down to 100.</p> <p>Set the following values for the threshold:</p> <ul style="list-style-type: none"> High Value: 150 High Value Rearm: 100 <p>This value enables you to be aware when a network performance problem starts to improve.</p>
Low Value	Enter the low threshold value. This value indicates the minimum value below which the metric will be considered to have violated the Nominal range.
Low Value Rearm	Enter the low value rearm for the threshold. For Packet Loss

Field Name	Description
	<p>metric, enter the Low Rearm Value in percentage.</p> <p>The low value rearm is used to indicate the end of the low threshold state and NNM iSPI Performance for QA clears the incident once it reaches above this value.</p> <p>The low value rearm must be greater than the low value.</p> <p>Example</p> <p>For the Mean Opinion Score (MOS) you must generate an incident when the MOS score is 3 and clear the incident when the score is improved to 4.5.</p> <p>Set the following values for the threshold:</p> <ul style="list-style-type: none"> • Low Value: 3 • Low Value Rearm: 4.5 <p>This value enables you to be aware when a network performance problem starts to improve.</p>

The following field appears, if you have selected the Type as Count-Based:

Field Name	Description
Trigger Count	Specify after how many consecutive threshold violations NNM iSPI Performance for QA must alert the operator by transitioning the threshold state to  High or  Low accordingly.

The following fields appear if you selected the Type as Time-Based:

Field Name	Description
High Duration	<p>Designate the minimum time within which the metric value must remain in the High range.</p> <p>For example if you specify this value to be 20 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 minutes.</p> <p>You define the high threshold value in the High Value field.</p> <p>The High Duration should be equal to or greater than the associated Polling Interval setting, because that is how often NNM iSPI Performance for QA provides a data point..</p>
High Duration Window	<p>Designate the window of time within which the High Duration criteria must be met.</p> <p>To enable this setting, the value must be:</p>

Field Name	Description
	<ul style="list-style-type: none"> • greater than 0 (zero) • the same as or greater than the High Duration value <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p> <p>For example, if you specify this value to be 30 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 out of 30 minutes.</p>



The following fields appear if you have selected the Type as Time-Based and the metric as MOS:

<p>Low Duration</p>	<p>Designate the minimum time within which the metric value must remain in the Low range.</p> <p>For example if you specify this value to be 20 minutes for MOS metric, NNM iSPI Performance for QA considers the threshold to be violated if the MOS is low for 20 minutes.</p> <p>You define the low threshold value in the Low Value field.</p> <p>The polling interval should be less than or equal to the Low Duration.</p>
<p>Low Duration Window</p>	<p>Designate the window of time within which the Low Duration criteria must be met.</p> <p>For example, if you specify this value to be 30 minutes for MOS metric, NNM iSPI Performance for QA considers the threshold to be violated if the MOS is low for 20 out of 30 minutes.</p> <p>To enable this setting, the value must be:</p> <ul style="list-style-type: none"> • greater than 0 (zero) • the same as or greater than the Low Duration value <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p>

5. Select the following to generate an incident when the time-based threshold or count-based threshold value is violated:

Field Name	Description
Generate Incident	Select this option if you want NNM iSPI Performance for QA to generate an incident for count-based or time-based threshold violations. By default this option is selected.

6. Use any one of the following options to complete the task:

Icons	Description
 Close	Closes the Add Threshold Configuration form without saving the threshold information you have entered.
 Save and Close	Saves the threshold information and closes the Threshold Configuration form


7. Click  **Refresh** to view the changes.

8. Click  **Save** or  **Save and Close** in the Threshold Configuration form.

Make sure that you click  **Save** or  **Save and Close** in the Threshold Configuration form.

Creating QA Group Baseline Threshold Settings

To add a new baseline setting configuration:

1. Specify all the mandatory fields when [adding QA group threshold settings](#).
2. Click  **New** in the **Baseline Settings** tab. The Add Baseline Settings form opens.
3. Specify the following to configure the baseline deviation settings:



Field Name	Description
Metric	Select the metric for which you require to configure baseline deviation settings. The valid metrics for baseline deviation setting configuration are as below: <ul style="list-style-type: none"> • RTT (ms) • RTT (microS) • Two Way Jitter (microS) • Two Way Packet Loss (%) • MOS


4. After you select the metric, the list of fields relevant to the selected metric appear. You can

specify the following values to configure the baseline deviation settings:

Field Name	Description
Upper Baseline Limit Enabled	<p>If enabled, NNM iSPI Performance for QA uses the Upper Baseline Limit attribute value to determine the number of standard deviations above the average that defines the upper baseline limit.</p> <p>If disabled, NNM iSPI Performance for QA does not define the upper baseline limit.</p> <p>This field is not applicable to MOS metric.</p>
Upper Baseline Limit Deviations - Above Average	<p>Enter the number of standard deviation s above the average values that NNM iSPI Performance for QA should use to determine the upper baseline limit.</p> <p>This field is not applicable to MOS metric.</p>
Lower Baseline Limit Enabled	<p>If enabled, NNM iSPI Performance for QA uses the Lower Baseline Limit attribute value to determine the number of standard deviations below the average that defines the lower baseline limit.</p> <p>If disabled, NNM iSPI Performance for QA does not define the lower baseline limit.</p> <p>This field is applicable to MOS metric only.</p>
Lower Baseline Limit Deviations - Below Average	<p>Enter the number of standard deviation below the average values that NNM iSPI Performance for QA should use to determine the lower baseline limit.</p> <p>This field is applicable to MOS metric only.</p>
Duration	<p>The minimum time for which the standard deviation must persist to deviate from the configured Baseline Range before the baseline state transitions to Abnormal Range and generates an incident.</p> <p>The Polling Interval should be less than or equal to the Duration.</p>
Window Duration	<p>The window duration within which the Upper Baseline Limit or Lower Baseline Limit Deviation criteria must be met.</p> <p>The value must be greater than 0 (zero) and can be the same as the Duration value.</p> <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p>

5. Use any one of the following options to complete the task:

Icons	Description
 Close	Closes the Add Baseline Settings form without saving the baseline setting information you have entered.
 Save and Close	Saves the baseline setting information and closes the Add Baseline Settings form


6. Click  **Save and Close** in the Add Baseline Settings form to save the baseline setting information.

7. Click  **Save** or  **Save and Close** in the Threshold Configuration form.

Make sure you click **Save** or  **Save and Close** in the Threshold Configuration form.

Editing QA Group Threshold Settings

To edit the QA Group threshold settings:

1. [Launch the Threshold Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Threshold Configuration** > **Probes** > **Sites/QA Group**. The Threshold Configuration form opens.
2. Select the threshold configuration settings to modify, and click  **Edit** in the Threshold Configuration form panel. The edit threshold configuration form opens.

When you edit the QA Group threshold configuration settings, NNM iSPI Performance for QA enables you to edit only the metric values, and does not enables you to edit the following fields:

- Threshold type
- Order
- QA Group
- Service





If you want to edit the above mentioned fields, delete the existing configuration settings and configure a new threshold setting, based on your requirements.

3. Follow the steps for [Editing an Existing Threshold](#) to modify the metric values.






You can view the two tabs; **Threshold Settings** and **Baseline Settings**.

You can perform the following tasks when you click on the **Threshold Settings** tab:

Icons	Description
 New	Creates QA Group threshold.


Icons	Description
 Edit	Edits QA Group threshold.
 Delete	Deletes QA Group threshold.
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data.
 Delete All	Deletes all QA Group thresholds

You can perform the following tasks when you click on the **Baseline Settings** tab:

Icons	Description
 New	Creates QA Group baseline threshold setting
 Edit	Edits QA Group baseline threshold settings
 Delete	Deletes QA Group baseline threshold settings
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data
 Delete All	Deletes all QA Group baseline threshold settings

Editing QA Group Threshold Setting

To edit an existing threshold setting:

1. Specify all the mandatory fields when [editing QA group threshold settings](#).
2. Select the metric, and click  **Edit** in the **Threshold Settings** tab.



The Edit Threshold Settings form opens.

You cannot edit the metric type and threshold type (Time-based or Count-based). If you want to edit the metric type or threshold type (Time-based or Count-based), delete the existing configuration settings and configure a new threshold settings, based on your requirements

3. You can specify the following values to edit the threshold:

Field Name	Description
High Value	<p>Enter the threshold value. This value indicates the maximum value above which the metric will be considered to have violated the Nominal range. For Packet Loss metric, enter the High Value in percentage.</p>
High Value Rearm	<p>Enter the high value rearm for the threshold. For Packet Loss metric, enter the High Value Rearm in percentage.</p> <p>The High Value Rearm is used to indicate the end of the high threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value.</p> <p>The high value rearm must always be lower than the high value.</p> <p>Example</p> <p>For the Round Trip Time (RTT) you must generate an incident when the RTT is 150 and clear the incident when the RTT value comes down to 100.</p> <p>Set the following values for the threshold:</p> <ul style="list-style-type: none"> • High Value: 150 • High Value Rearm: 100 <p>This value enables you to be aware when a network performance problem starts to improve.</p>
Low Value	<p>Enter the low threshold value. This value indicates the minimum value below which the metric will be considered to have violated the Nominal range.</p>
Low Value Rearm	<p>Enter the low value rearm for the threshold. For Packet Loss metric, enter the Low Rearm Value in percentage.</p> <p>The low value rearm is used to indicate the end of the low threshold state and NNM iSPI Performance for QA clears the incident once it reaches above this value.</p> <p>The low value rearm must be greater than the low value.</p> <p>Example</p> <p>For the Mean Opinion Score (MOS) you must generate an incident when the MOS score is 3 and clear the incident when the score is improved to 4.5.</p> <p>Set the following values for the threshold:</p> <ul style="list-style-type: none"> • Low Value: 3 • Low Value Rearm: 4.5 <p>This value enables you to be aware when a network performance problem starts to improve.</p>

The following field appears, if you have selected the Type as Count-Based:

Field Name	Description
Trigger Count	Specify after how many consecutive threshold violations NNM iSPI Performance for QA must alert the operator by transitioning the threshold state to  High or  Low accordingly.

The following fields appear if you selected the Type as Time-Based:

Field Name	Description
High Duration	<p>Designate the minimum time within which the metric value must remain in the High range.</p> <p>For example if you specify this value to be 20 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 minutes.</p> <p>You define the high threshold value in the High Value field.</p> <p>The High Duration should be equal to or greater than the associated Polling Interval setting, because that is how often NNM iSPI Performance for QA provides a data point..</p>
High Duration Window	<p>Designate the window of time within which the High Duration criteria must be met.</p> <p>To enable this setting, the value must be:</p> <ul style="list-style-type: none"> • greater than 0 (zero) • the same as or greater than the High Duration value <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p> <p>For example, if you specify this value to be 30 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 out of 30 minutes.</p>

The following fields appear if you have selected the Type as Time-Based and the metric as MOS:



Low Duration	<p>Designate the minimum time within which the metric value must remain in the Low range.</p> <p>For example if you specify this value to be 20 minutes for MOS metric, NNM iSPI Performance for QA considers the threshold to be violated if the MOS is low for 20 minutes.</p> <p>You define the low threshold value in the Low Value field.</p>
--------------	--

	The polling interval should be less than or equal to the Low Duration.
Low Duration Window	<p>Designate the window of time within which the Low Duration criteria must be met.</p> <p>For example, if you specify this value to be 30 minutes for MOS metric, NNM iSPI Performance for QA considers the threshold to be violated if the MOS is low for 20 out of 30 minutes.</p> <p>To enable this setting, the value must be:</p> <ul style="list-style-type: none"> • greater than 0 (zero) • the same as or greater than the Low Duration value <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p>

4. Select the following to generate an incident when the time-based threshold or count-based threshold value is violated:

Field Name	Description
Generate Incident	Select this option if you want NNM iSPI Performance for QA to generate an incident for count-based or time-based threshold violations. By default this option is selected.

5. Use any one of the following options to complete the task:

Icons	Description
 Close	Closes the Edit Threshold Configuration form without saving the threshold information you have entered.
 Save and Close	Saves the threshold information and closes the Threshold Configuration form

6. Click  **Refresh** to view the changes.


7. Click  **Save** or  **Save and Close** in the Threshold Configuration form.

Make sure you click  **Save** or  **Save and Close** in the Threshold Configuration form, to save the settings that you have edited.

Editing QA Group Baseline Threshold Settings

To edit the threshold for baseline settings:

1. [Launch the Threshold Configuration form.](#)
 - a. Select **Configuration workspace > Quality Assurance Configuration Console**. The

- configuration console opens.
- b. In the **Configuration** workspace, select **Threshold Configuration > Probes > Sites/QA Group**. The Threshold Configuration form opens.
2. Select the configured threshold to modify, and Click  **Edit** in the **Baseline Settings** tab. The Edit Baseline Settings form opens.

When you edit the QA Group baseline threshold configuration settings, NNM iSPI Performance for QA enables you to edit only the metric values, and does not enables you to edit the following fields:


- Threshold type
- Order
- QA Group
- Service

If you want to edit the above mentioned fields, delete the existing configuration settings and configure a new threshold setting, based on your requirements.

3. Follow the steps for [editing QA group baseline threshold setting](#), to modify the metric values.

Editing QA Group Baseline Threshold Settings

To edit the threshold for baseline settings:

1. Specify all the mandatory fields in the [Editing QA Group Baseline Threshold Settings](#).
2. Select the metric in the **Baseline Settings** tab, and Click  **Edit**. The Edit Baseline Settings form opens.



You cannot edit the metric type and threshold type (Time-based or Count-based). If you want to edit the metric type or threshold type (Time-based or Count-based), delete the existing configuration settings and configure a new threshold settings, based on your requirements.




3. You can specify the following to edit the baseline deviation settings:

Field Name	Description
Upper Baseline Limit Enabled	<p>If enabled, NNM iSPI Performance for QA uses the Upper Baseline Limit attribute value to determine the number of standard deviations above the average that defines the upper baseline limit.</p> <p>If disabled, NNM iSPI Performance for QA does not define the upper baseline limit.</p> <p>This field is not applicable to MOS metric.</p>
Upper Baseline Limit Deviations - Above Average	<p>Enter the number of standard deviation s above the average values that NNM iSPI Performance for QA should use to determine the upper baseline limit.</p>

Field Name	Description
	This field is not applicable to MOS metric.
Lower Baseline Limit Enabled	<p>If enabled, NNM iSPI Performance for QA uses the Lower Baseline Limit attribute value to determine the number of standard deviations below the average that defines the lower baseline limit.</p> <p>If disabled, NNM iSPI Performance for QA does not define the lower baseline limit.</p> <p>This field is applicable to MOS metric only.</p>
Lower Baseline Limit Deviations - Below Average	<p>Enter the number of standard deviation below the average values that NNM iSPI Performance for QA should use to determine the lower baseline limit.</p> <p>This field is applicable to MOS metric only.</p>
Duration	<p>The minimum time for which the standard deviation must persist to deviate from the configured Baseline Range before the baseline state transitions to Abnormal Range and generates an incident.</p> <p>The Polling Interval should be less than or equal to the Duration.</p>
Window Duration	<p>The window duration within which the Upper Baseline Limit or Lower Baseline Limit Deviation criteria must be met.</p> <p>The value must be greater than 0 (zero) and can be the same as the Duration value.</p> <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p>

4. Use any one of the following options to complete the task:




Icons	Description
 Close	Closes the Edit Baseline Settings form without saving the baseline setting information you have entered.
 Save and Close	Saves the baseline setting information and closes the Edit Baseline Settings form

5. Click  **Save and Close** in the Edit Baseline Settings form to save the baseline setting information.
6. Click  **Save** or  **Save and Close** in the Threshold Configuration form.

Make sure you click **Save** or  **Save and Close** in the Threshold Configuration form, to save the settings that you have edited.

Deleting QA Group Thresholds




To delete an existing QA Group for QA Probe threshold:

1. [Launch the Threshold Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Threshold Configuration** > **Probes** > **Sites/QA Group**. The Threshold Configuration form opens.
2. Select one or more configured QA Group threshold settings in the **Threshold Settings** panel and click  **Delete**.
or
Click  **Delete All** to delete all thresholds.
3. Click  **Refresh** in the Threshold Configuration panel to view the changes.

However, NNM iSPI Performance for QA does not delete the incidents that are already generated for an existing threshold.

Deleting QA Group Baseline Thresholds


To delete an existing QA Group for QA Probe baseline threshold:

1. [Launch the Threshold Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Threshold Configuration** > **Probes** > **Sites/QA Group**. The Threshold Configuration form opens.
2. Select **Baseline Settings** tab.
3. Select one or more threshold settings in the **Baseline Settings** panel, and Click  **Delete**.
or
Click  **Delete All** to delete all thresholds.
4. Click  **Refresh** in the Baseline panel to view the changes.

However, NNM iSPI Performance for QA does not delete the incidents that are already generated for an existing threshold.

Importing QA Group Thresholds

To import the existing QA Group for QA Probe thresholds configurations from an XML file:

1. [Launch the Threshold Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Threshold Configuration** > **Probes** > **Sites/QA Group**. The Threshold Configuration form opens.
2. Click  **Import**.
3. In the user prompt dialog, enter the file name from where you want to import the QA Groups for QA Probe thresholds configuration information.
You must enter the file name with full path information; for example, C:\temp\threshold_conf.xml
4. Click **OK** in the user prompt dialog.
If a threshold is already defined and displayed in the Threshold Configuration panel, the import utility does not import the configuration information for this threshold from the XML file.

You can also import the QA Groups for QA Probe thresholds configuration information using the following command line utility:

Linux: \$NnmInstallDir/bin/nmsgathresholdconfigutil.ovpl -u <username> -p <password> -import -type qaprobe <filename>

Windows: %NnmInstallDir%\bin\nmsgathresholdconfigutil.ovpl -u <username> -p <password> -import -type qaprobe <filename>

If the threshold import fails, check the following log files:


Linux: \$NnmDataDir/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Note: -u <username> -p <password> are optional parameters.

Exporting QA Group Thresholds

To export the existing QA Group for QA Probe threshold configurations to an XML file:

1. [Launch the Threshold Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Threshold Configuration** > **Probes** > **Sites/QA Group**. The Threshold Configuration form opens.
2. Click  **Export**.
3. Type the file name where you want to export the existing QA Groups for QA Probe threshold configurations in the user prompt dialog.
You must type the file name with full path information; for example, C:\temp\threshold_conf.xml

If you type the XML file name without entering the absolute path, by default the file gets saved in the following directory:

Linux: \$NnmDataDir/shared/qa/conf

Windows : %NnmDataDir%\shared\qa\conf

4. Click **OK** in the user prompt dialog.

You can also export the existing QA Groups for QA Probe threshold configurations using the following command line utility:

Linux: \$NnmInstallDir/bin/nmsgathresholdconfigutil.ovpl -u <username> -p <password> -export -type qaprobe <filename>

Windows: %NnmInstallDir%\bin\nmsgathresholdconfigutil.ovpl -u <username> -p <password> -export -type qaprobe <filename>

The threshold export utility does not export a threshold unless the threshold is associated with a QA Group.

If the threshold export fails, check the following log files:

Linux: \$NnmDataDir/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Note: -u <username> -p <password> are optional parameters.

Configuring Site Thresholds

To configure a threshold for a site, you must have a source site, but may not have a destination site. If you do not assign a destination site to the threshold, the threshold is applied to all the QA probes run from the source site.

You can configure thresholds for the following Quality Assurance metrics derived from the QA probes configured for an existing site:

- Round Trip Time (RTT)
- Jitter
- Packet Loss (Can be from source to destination, and from destination to source.)
- Mean Opinion Score (MOS)

Note: For configuring thresholds for probes, it is recommended to use the QA group-based threshold configuration than the site-based threshold configuration. For more information about configuring thresholds for QA groups, see ["Adding QA Group Threshold Configuration" on page 235](#)

NNM iSPI Performance for QA performs the following actions if a threshold is breached:

- Sets the QA probe status to Major.
- Creates an incident for the violated threshold.
- Sends the threshold violation details to the Network Performance Server for generating reports.
- Retains the threshold state as Nominal, or sets the threshold state to High or Low depending on the count-based, or time-based threshold configuration.

For information about overriding thresholds of probes specific to a site, see "[Configuring Probe Thresholds](#)" on page 213.

In a GNM environment, the global manager receives the threshold states from the sites in the regional managers. You **cannot** configure thresholds for remote sites. The thresholds configured for the sites of the global managers are not applicable for the sites of regional managers.

You can monitor the network performance and generate an incident based on the count-based threshold or time-based threshold configuration.

You can only configure threshold for a combination of a site, service, and metric.

Threshold Configurations

Count-Based Threshold Configuration

You can generate an incident based on the count or number of consecutive times a metric violates the threshold value. You can define this count in the Threshold Configuration form.

Time-Based Threshold Configuration

Time-Based threshold configuration enables you to raise an alert when the threshold breached state persists for more than a specific time period. This is derived by specifying X as the duration of time in minutes when the metric is in a threshold breached state within Y number of minutes specified in the sliding window.

Example for Time-Based Threshold Configuration

Consider a scenario, where the polling interval is 5 minutes; High duration is 10 minutes; and High Duration Window is 60 minutes. In this scenario, an incident is generated whenever the High Duration exceeds 10 minutes within the 60 minute duration. NNM iSPI Performance for QA uses a sliding window wherein each time the High Duration (10 minutes) is reached, NNM iSPI Performance for QA drops the oldest polled value (first 5 minutes) and adds the most recent (between 60 to 65 minutes). This procedure continues and enables you to determine time-based threshold violation.

You can make utmost use of the Time-Based threshold violation by ensuring that the duration specified in the sliding window is greater than or equal to the polling interval.

Baseline Settings Configuration

Baseline Deviation Settings Configuration

Apart from the time-based and count-based threshold configuration, you can also do a [baseline monitoring](#) based on the baseline deviation setting configuration in NNM iSPI Performance for QA. You can do a baseline deviation setting configuration for the selected site, service, and metric. An incident is generated and the baseline state transitions to Abnormal Range only if it meets all the criteria listed below:

- Exceeds the count or the number of standard deviation that is above the average value for the metric, or exceeds the count or the number of standard deviation that is below the average value for the metric. This count is specified in the Upper Baseline Limit Deviations or Lower Baseline Limit Deviations for the selected metric in the baseline deviation settings configuration.

- Exceeds the duration for which the upper or lower baseline deviation persists in the specified sliding window duration

Note: HP recommends that you have the probes with same frequency in a QA site for the Baseline Threshold feature to work effectively.

Adding Threshold Configuration

To add a new threshold configuration:





1. [Launch the Threshold Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Threshold Configuration** > **Probes** > **Sites/QA Group**. The Threshold Configuration form opens.
2. Click *** New** in the **Threshold Configuration** panel.
The Add Threshold Configuration form opens.
3. Select **Site** in Threshold Type field.
4. Specify the following information in the **Threshold Configuration** panel:

Field Name	Description
Threshold Type	In the Threshold Type, select Site Based .
Order	Specify a numeric value. NNM iSPI Performance for QA checks the configuration settings in the order you define (lowest number first)
Source Site	Select the name of the source site. This field is mandatory.
Destination Site	Select the destination site for the QA probes. This field is optional.
Service	The type of the discovered QA probe. This field is mandatory. NNM iSPI Performance for QA recognizes the following QA probe types: <ul style="list-style-type: none">• UDP Echo• ICMP Echo• UDP• TCP Connect• HTTP• HTTPS





Field Name	Description
	<ul style="list-style-type: none"> • VoIP • DNS • DHCP • Oracle • ICMP Jitter

You can view the two tabs; Threshold Settings and Baseline Settings.

5. You can perform the following tasks when you click on the **Threshold Settings** tab.

Icon	Description
 New	Adds threshold settings for the site.
 Delete	Deletes the selected threshold settings for the site.
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data.
 Delete All	Deletes all the thresholds configured for the site.

6. You can perform the following tasks when you click on the **Baseline Settings** tab.

Icon	Description
 New	Adds baseline settings for the site.
 Delete	Deletes the selected baseline settings for the site.
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data.
 Delete All	Deletes all the baseline settings configured for the site.

Adding Threshold Settings

To add a new threshold setting:

1. Make sure that you selected the Source Site, and Service when [Adding Threshold Configuration](#).
2. Click

*** New in the Threshold Settings tab.**

The Add Threshold Settings form opens.

- Specify the following to configure the threshold settings:



Field Name	Description
Type	Select the type of threshold violation. The valid types are Count-Based and Time-Based .
Metric	Select the metric for which you are configuring the threshold. The metrics are populated based on the service. For information about the metrics for each service type, see "Supported Threshold Configuration Metrics" on page 299 .

- After you select the metric to configure the threshold, the list of fields relevant to the selected metric appear. You can specify the following values to configure the new threshold:

Field Name	Description
High Value	Enter the threshold value. This value indicates the maximum value above which the metric will be considered to have violated the Nominal range. For Packet Loss metric, enter the High Value in percentage.
High Value Rearm	<p>Enter the high value rearm for the threshold. For Packet Loss metric, enter the High Value Rearm in percentage.</p> <p>The High Value Rearm is used to indicate the end of the high threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value.</p> <p>The high value rearm must always be lower than the high value.</p> <p>Example</p> <p>For the Round Trip Time (RTT) you must generate an incident when the RTT is 150 and clear the incident when the RTT value comes down to 100.</p> <p>Set the following values for the threshold:</p> <ul style="list-style-type: none"> High Value: 150 High Value Rearm: 100 <p>This value enables you to be aware when a network performance problem starts to improve.</p>
Low Value	Enter the low threshold value. This value indicates the minimum value below which the metric will be considered to have violated the Nominal range.
Low Value Rearm	Enter the low value rearm for the threshold. For Packet Loss

Field Name	Description
	<p>metric, enter the Low Rearm Value in percentage.</p> <p>The low value rearm is used to indicate the end of the low threshold state and NNM iSPI Performance for QA clears the incident once it reaches above this value.</p> <p>The low value rearm must be greater than the low value.</p> <p>Example</p> <p>For the Mean Opinion Score (MOS) you must generate an incident when the MOS score is 3 and clear the incident when the score is improved to 4.5.</p> <p>Set the following values for the threshold:</p> <ul style="list-style-type: none"> • Low Value: 3 • Low Value Rearm: 4.5 <p>This value enables you to be aware when a network performance problem starts to improve.</p>

The following field appears, if you selected the Type as Count-Based:

Field Name	Description
Trigger Count	<p>Specify after how many consecutive threshold violations NNM iSPI Performance for QA must alert the operator by transitioning the threshold state to  High or  Low accordingly.</p>

The following fields appear if you selected the Type as Time-Based:

Field Name	Description
High Duration	<p>Designate the minimum time within which the metric value must remain in the High range.</p> <p>For example if you specify this value to be 20 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 minutes.</p> <p>You define the high threshold value in the High Value field.</p> <p>The High Duration should be equal to or greater than the associated Polling Interval setting, because that is how often NNM iSPI Performance for QA provides a data point..</p>
High Duration Window	<p>Designate the window of time within which the High Duration criteria must be met.</p> <p>To enable this setting, the value must be:</p> <ul style="list-style-type: none"> • greater than 0 (zero)

Field Name	Description
	<ul style="list-style-type: none"> the same as or greater than the High Duration value <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p> <p>For example, if you specify this value to be 30 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 out of 30 minutes.</p>



The following fields appear if you selected the Type as Time-Based and the metric as MOS:




Low Duration	<p>Designate the minimum time within which the metric value must remain in the Low range.</p> <p>For example if you specify this value to be 20 minutes for MOS metric, NNM iSPI Performance for QA considers the threshold to be violated if the MOS is low for 20 minutes.</p> <p>You define the low threshold value in the Low Value field.</p> <p>The polling interval should be less than or equal to the Low Duration.</p>
Low Duration Window	<p>Designate the window of time within which the Low Duration criteria must be met.</p> <p>For example, if you specify this value to be 30 minutes for MOS metric, NNM iSPI Performance for QA considers the threshold to be violated if the MOS is low for 20 out of 30 minutes.</p> <p>To enable this setting, the value must be:</p> <ul style="list-style-type: none"> greater than 0 (zero) the same as or greater than the Low Duration value <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p>



- Select the following to generate an incident when the time-based threshold or count-based threshold value is violated:

Field Name	Description
Generate Incident	Select this option if you want NNM iSPI Performance for QA to generate an incident. By default this option is selected.

- Use any one of the following options to complete the task:

Icons	Description
 Close	Closes the Add Threshold Configuration form without saving the threshold information you have entered.
 Save and Close	Saves the threshold information and closes the Threshold Configuration form

- Click  **Refresh** to view the changes.
- Click  **Save** or  **Save and Close** in the Threshold Configuration form.

Caution: The new threshold is not saved unless you click  **Save** or  **Save and Close** in the Threshold Configuration form.

NNM iSPI Performance for QA applies the following rules when creating thresholds for a **site** using this form:

- You can create thresholds only for the existing sites.
- You must select a source site and service for the new threshold.
- You could select the destination site for the new threshold
- If you do not specify a destination site for the threshold, the threshold is applied to all the destination sites of the source sites.
- You cannot configure thresholds for remote sites.


Time-Based Threshold cannot be configured for QA probes, if the polling interval is greater than the High Duration or Low Duration value. A list of these QA Probes, the UUID, and other details can be viewed in the log file, which is available in the following directory:

Linux: \$NnmDataDir/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Adding Baseline Settings

To add a new baseline setting configuration:

- Make sure that you selected the Source Site, and Service in the [adding threshold configuration](#) .
- Click  **New** in the **Baseline Settings** tab. The Add Baseline Settings form opens.
- Specify the following to configure the baseline deviation settings:

Field Name	Description
Metric	Select the metric for which you require to configure baseline deviation settings. The valid metrics for baseline deviation setting configuration are as below: <ul style="list-style-type: none"> RTT (ms)



Field Name	Description
	<ul style="list-style-type: none"> • RTT (microS) • Two Way Jitter (microS) • Two Way Packet Loss (%) • MOS




4. After you select the metric, the list of fields relevant to the selected metric appear. You can specify the following values to configure the baseline deviation settings:



Field Name	Description
Upper Baseline Limit Enabled	<p>If enabled, NNM iSPI Performance for QA uses the Upper Baseline Limit attribute value to determine the number of standard deviations above the average that defines the upper baseline limit.</p> <p>If disabled, NNM iSPI Performance for QA does not define the upper baseline limit.</p> <p>This field is not applicable to MOS metric.</p>
Upper Baseline Limit Deviations - Above Average	<p>Enter the number of standard deviation s above the average values that NNM iSPI Performance for QA should use to determine the upper baseline limit.</p> <p>This field is not applicable to MOS metric.</p>
Lower Baseline Limit Enabled	<p>If enabled, NNM iSPI Performance for QA uses the Lower Baseline Limit attribute value to determine the number of standard deviations below the average that defines the lower baseline limit.</p> <p>If disabled, NNM iSPI Performance for QA does not define the lower baseline limit.</p> <p>This field is applicable to MOS metric only.</p>
Lower Baseline Limit Deviations - Below Average	<p>Enter the number of standard deviation below the average values that NNM iSPI Performance for QA should use to determine the lower baseline limit.</p> <p>This field is applicable to MOS metric only.</p>
Duration	<p>The minimum time for which the standard deviation must persist to deviate from the configured Baseline Range before the baseline state transitions to Abnormal Range and generates an incident.</p> <p>The Polling Interval should be less than or equal to the Duration.</p>

Field Name	Description
Window Duration	<p>The window duration within which the Upper Baseline Limit or Lower Baseline Limit Deviation criteria must be met.</p> <p>The value must be greater than 0 (zero) and can be the same as the Duration value.</p> <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p>

5. Use any one of the following options to complete the task:

Icon	Description
 Close	Closes the Add Baseline Settings form without saving the baseline setting information you have entered.
 Save and Close	Saves the baseline setting information and closes the Add Baseline Settings form.

6. Click  **Save and Close** in the Add Baseline Settings form to save the baseline setting information.
7. Click  **Save** or  **Save and Close** in the Threshold Configuration form.

The new baseline settings configuration is not saved unless you click  **Save** or  **Save and Close** in the Threshold Configuration form.

NNM iSPI Performance for QA applies the following rules while configuring baseline deviation settings for a **site** using this form:


- You can configure baseline settings only for the QA probes of the existing sites.
- You must select a source site, service, and metric to configure the baseline settings.
- Optionally, you can select the destination site
- If you do not specify a destination site for the baseline setting, the configuration is applied to all the QA probes of the destination sites from the source sites.
- You cannot configure baseline settings for remote sites.

Editing Threshold Configuration

To edit a threshold configuration:

1. [Launch the Threshold Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.

- b. In the **Configuration** workspace, select **Threshold Configuration > Probes > Sites/QA Group**. The Threshold Configuration form opens.

2. Select the threshold configuration settings to modify, and click  **Edit**.

The Edit Threshold Configuration form opens.

When you edit a QA Group threshold configuration setting, NNM iSPI Performance for QA enables you to edit only the metric values, and does not enables you to edit the following fields:






- Threshold Type
- Order
- Source Site
- Destination Site
- Service

If you want to edit the above mentioned fields, delete the existing configuration settings and configure a new threshold setting, based on your requirements.



3. Follow the steps given for [editing threshold settings](#) to modify the metric values.




You can view two tabs; **Threshold Settings** and **Baseline Settings**.

You can perform the following tasks when you click on the **Threshold Settings** tab.

Icon	Description
 New	Adds threshold settings for the site.
 Edit	Edits the selected threshold settings for the site.
 Delete	Deletes the selected threshold setting for the site.
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data.
 Delete All	Deletes all the threshold settings configured for the site.


You can perform the following tasks when you click on the **Baseline Settings** tab:

Icon	Description
 New	Adds baseline deviation settings for the site.
 Edit	Edits baseline deviation settings for the site.

Icon	Description
 Delete	Deletes the selected baseline deviation setting for the site.
 Refresh	Retrieves the last saved baseline deviation setting configuration from the database and displays the data.
 Delete All	Deletes all the baseline deviation settings configured for the site.

Editing Threshold Settings

To edit an existing threshold setting:

- Specify all the mandatory fields when [editing threshold configuration](#).
 - Select the metric, and click  **Edit** in the **Threshold Settings** tab.
 The Edit Threshold Settings form opens.

Caution: You cannot edit the metric type and threshold type (Time-based or Count-based). If you want to edit the metric type or threshold type (Time-based or Count-based), delete the existing configuration settings and configure a new threshold settings, based on your requirements.

- You can specify the following values to edit the threshold:



For probe based threshold configuration, you can view the threshold that was configured for the Remote QA probes, but you **cannot** configure thresholds for [Remote QA Probes](#)¹.

Field Name	Description
High Value	Enter the threshold value. This value indicates the maximum value above which the metric will be considered to have violated the Nominal range. For Packet Loss metric, enter the High Value in percentage.
High Value Rearm	<p>Enter the high value rearm for the threshold. For Packet Loss metric, enter the High Value Rearm in percentage.</p> <p>The High Value Rearm is used to indicate the end of the high threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value.</p> <p>The high value rearm must always be lower than the high value.</p> <p>Example</p> <p>For the Round Trip Time (RTT) you must generate an incident when the</p>

¹At Global server, the probes discovered and forwarded by regional servers are called as remote probes. You can manage threshold for these probes only at regional manager.

Field Name	Description
	<p>RTT is 150 and clear the incident when the RTT value comes down to 100.</p> <p>Set the following values for the threshold:</p> <ul style="list-style-type: none"> • High Value: 150 • High Value Rearm: 100 <p>This value enables you to be aware when a network performance problem starts to improve.</p>
Low Value	<p>Enter the low threshold value. This value indicates the minimum value below which the metric will be considered to have violated the Nominal range.</p>
Low Value Rearm	<p>Enter the low value rearm for the threshold. For Packet Loss metric, enter the Low Rearm Value in percentage.</p> <p>The low value rearm is used to indicate the end of the low threshold state and NNM iSPI Performance for QA clears the incident once it reaches above this value.</p> <p>The low value rearm must be greater than the low value.</p> <p>Example</p> <p>For the Mean Opinion Score (MOS) you must generate an incident when the MOS score is 3 and clear the incident when the score is improved to 4.5.</p> <p>Set the following values for the threshold:</p> <ul style="list-style-type: none"> • Low Value: 3 • Low Value Rearm: 4.5 <p>This value enables you to be aware when a network performance problem starts to improve.</p>

The following fields appear, if the Type is Count-Based, and you can modify the information if required

Field Name	Description
Trigger Count	<p>Specify after how many consecutive threshold violations NNM iSPI Performance for QA must alert the operator by transitioning the threshold state to  High or  Low accordingly.</p>

The following fields appear if the Type is Time-Based, and you can modify the information if required:

Field Name	Description
High Duration	<p>Designate the minimum time within which the metric value must remain in the High range.</p> <p>For example if you specify this value to be 20 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 minutes.</p> <p>You define the high threshold value in the High Value field.</p> <p>The High Duration should be equal to or greater than the associated Polling Interval setting, because that is how often NNM iSPI Performance for QA provides a data point..</p>
High Duration Window	<p>Designate the window of time within which the High Duration criteria must be met.</p> <p>To enable this setting, the value must be:</p> <ul style="list-style-type: none"> • greater than 0 (zero) • the same as or greater than the High Duration value <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p> <p>For example, if you specify this value to be 30 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 out of 30 minutes.</p>

The following fields appear, if you selected the Type as Time-Based and the metric as MOS:

You can modify the information if required.



Low Duration	<p>Designate the minimum time within which the metric value must remain in the Low range.</p> <p>For example if you specify this value to be 20 minutes for MOS metric, NNM iSPI Performance for QA considers the threshold to be violated if the MOS is low for 20 minutes.</p> <p>You define the low threshold value in the Low Value field.</p> <p>The polling interval should be less than or equal to the Low Duration.</p>
Low Duration Window	<p>Designate the window of time within which the Low Duration criteria must be met.</p> <p>For example, if you specify this value to be 30 minutes for MOS</p>




	<p>metric, NNM iSPI Performance for QA considers the threshold to be violated if the MOS is low for 20 out of 30 minutes.</p> <p>To enable this setting, the value must be:</p> <ul style="list-style-type: none"> • greater than 0 (zero) • the same as or greater than the Low Duration value <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p>
--	--



3. Select the following to generate an incident when the time-based threshold or count-based threshold value is violated:

Field Name	Description
Generate Incident	Select this option if you want NNM iSPI Performance for QA to generate an incident for count-based or time-based threshold violations. By default this option is selected.

4. Use any one of the following options to complete the task:

Icons	Description
 Close	Closes the Add Threshold Configuration form without saving the threshold information you have entered
 Save and Close	Saves the threshold information and closes the Threshold Configuration form

5. Click  **Refresh** in the Threshold Settings panel to view the changes.
6. Click  **Save** or  **Save and Close** in the Threshold Configuration form.

Note: The changes you have made in the threshold is not saved unless you click  **Save** or  **Save and Close** in the Threshold Configuration form.


NNM iSPI Performance for QA applies the following rules while updating thresholds:

- You can define thresholds only for the existing sites.
- Any modification in the threshold directly updates the state poller.

Time-Based Threshold cannot be configured for QA probes, if the polling interval is greater than the High Duration or Low Duration value. A list of these QA Probes, the UUID, and other details can be viewed in the log file, which is available in the following directory:

Linux: \$NnmDataDir/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Note: You can select all the threshold configured settings and click  **Edit** option, but edit form will open for only one threshold group.

Editing Baseline Settings

To edit a baseline setting configuration:

1. Make sure that you selected the Source Site, and Service when [editing threshold configuration](#) if you are launching the form from Site Wide threshold configuration. You can ignore this step if you are launching this form from Probe-based threshold configuration.

2. Select the baseline settings, and click  **Edit** in the **Baseline Settings** panel.

The Edit Baseline Settings form opens.

3. In the **Baseline Deviations Settings** panel:

- a. You can view the following details:

Field Name	Description
Metric	The metric for which you require to edit the baseline deviations settings configuration.



- b. You can edit the following baseline deviation settings configuration:


The following fields appear depending on the metric:



Field Name	Description
Upper Baseline Limit Enabled	If enabled, NNM iSPI Performance for QA uses the Upper Baseline Limit attribute value to determine the number of standard deviations above the average that defines the upper baseline limit. If disabled, NNM iSPI Performance for QA does not define the upper baseline limit. This field is not applicable to MOS metric.
Upper Baseline Limit Deviations - Above Average	Enter the number of standard deviation s above the average values that NNM iSPI Performance for QA should use to determine the upper baseline limit. This field is not applicable to MOS metric.
Lower Baseline Limit Enabled	If enabled, NNM iSPI Performance for QA uses the Lower Baseline Limit attribute value to determine the number of standard deviations below the average that defines the lower baseline limit. If disabled, NNM iSPI Performance for QA does not define the lower baseline limit. This field is applicable to MOS metric only.



Field Name	Description
Lower Baseline Limit Deviations - Below Average	Enter the number of standard deviation below the average values that NNM iSPI Performance for QA should use to determine the lower baseline limit. This field is applicable to MOS metric only.
Duration	The minimum time for which the standard deviation must persist to deviate from the configured Baseline Range before the baseline state transitions to Abnormal Range and generates an incident. The Polling Interval should be less than or equal to the Duration.
Window Duration	The window duration within which the Upper Baseline Limit or Lower Baseline Limit Deviation criteria must be met. The value must be greater than 0 (zero) and can be the same as the Duration value. The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.

4. Use any one of the following options to complete the task:

Icon	Description
 Close	Closes the Edit Baseline Settings form without saving the baseline setting information you have entered.
 Save and Close	Saves the baseline setting information and closes the Edit Baseline Settings form

5. Click  **Save and Close** in the Edit Baseline Settings form to save the baseline setting information.

6. Click  **Save** or  **Save and Close** in the Site Wide Threshold Configuration form.

The new baseline settings configuration is not be saved unless you click  **Save** or  **Save and Close** in the Threshold Configuration form.




NNM iSPI Performance for QA applies the following rules while configuring baseline deviation settings for a **site** using this form:

- You can configure baseline settings only for the QA probes of the existing sites.
- You must select a source site and service to configure the baseline settings.
- Optionally, you could select the destination site.
- If you do not specify a destination site for the baseline setting, the configuration is applied to all the


- QA probes of the destination sites from the source sites.
- You cannot configure baseline settings for remote sites.

Deleting Thresholds

To delete an existing threshold:

1. [Launch the Threshold Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Threshold Configuration** > **Probes** > **Sites/QA Group**. The Threshold Configuration form opens.
2. Select a threshold in the **Threshold Settings** panel and click  **Delete**.
or
Click  **Delete All** to delete all thresholds.
3. Click  **Refresh** in the Threshold Settings panel to view the changes.

The following changes occur after deleting a site based threshold configuration:

The selected thresholds configured for the metrics of the site are deleted and the threshold state is set to  Threshold Not Set for the metric in the site. If any probe based configuration exists for the metric, the deletion of the site based threshold configuration has no impact on the probe based threshold configuration. The QA Probe status for the probes in the site is set to the most severe status. The incidents and conclusions are updated accordingly.

Example 1

Consider the following scenario:

Before Deleting the Threshold(s) Configured for the Site:

QA Probe Status :  Major

Threshold State:  High

Note: The threshold state is high for RTT and Packet Loss

Conclusion: RttThresholdStateHigh, TwoWayPktLossThresholdStateHigh, RTTAbnormal

After Deleting the Threshold(s) Configured for the Site:

QA Probe Status :  Major

Threshold State:  Threshold Not Set

Note: The threshold state is set to Threshold Not Set for RTT and Packet Loss.

Conclusion: RTTAbnormal

The QA Probe Status for the probes in the site is still set to Major as the Baseline State is in the Abnormal Range.

Example 2

Consider the following scenario:

Before Deleting the Threshold(s) Configured for the Site:

QA Probe Status :  Major

Threshold State:  High

Conclusion: [TestUp¹](#), RttThresholdStateHigh,TwoWayPktLossThresholdStateHigh

Deleting the Threshold(s) Configured for the Site:

QA Probe Status :  Normal

Threshold State:  Threshold Not Set

Conclusion: [TestUp²](#)

Exporting Thresholds

To export the existing threshold configurations to an XML file:

1. [Launch the Threshold Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Threshold Configuration** > **Probes** > **Sites/QA Group**. The Threshold Configuration form opens.

2. Click  **Export**.

3. Type the file name where you want to export the existing threshold configuration in the user prompt dialog.

You must type the file name with full path information; for example, C:\temp\threshold_conf.xml

If you type the XML file name without entering the absolute path, by default the file gets saved in the following directory:

Linux: \$NnmDataDir/shared/qa/conf

Windows : %NnmDataDir%\shared\qa\conf

4. Click **OK** in the user prompt dialog.

You can also export the existing threshold configuration using the following command line utility:

Linux: \$NnmInstallDir/bin/nmsqathresholdconfigutil.ovpl -u <username> -p <password> -export <filename>

Windows: %NnmInstallDir%\bin\nmsqathresholdconfigutil.ovpl -u <username> -p <password> -export <filename>

¹When both Administrative and Operational states are up.

²When both Administrative and Operational states are up.

The threshold export utility does not export a threshold unless the threshold is associated with at least one site.

If the threshold export fails, check the following log files:

Linux: \$NnmDataDir/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Note: -u <username> -p <password> are optional parameters.

Importing Thresholds

To import threshold configurations from an XML file:

1. [Launch the Threshold Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Threshold Configuration** > **Probes** > **Sites/QA Group**. The Threshold Configuration form opens.

2. Click  **Import**.

3. In the user prompt dialog, enter the file name from where you want to import the threshold configuration information.

You must enter the file name with full path information; for example, C:\temp\threshold_conf.xml

4. Click **OK** in the user prompt dialog.

If a threshold is already defined and displayed in the Site Wide Threshold Settings panel, the import utility does not import the configuration information for this threshold from the XML file.

You can also import threshold configuration information using the following command line utility:

Linux: \$NnmInstallDir/bin/nmsqathresholdconfigutil.ovpl -u <username> -p <password> -import <filename>

Windows: %NnmInstallDir%\bin\nmsqathresholdconfigutil.ovpl -u <username> -p <password> -import <filename>

If the threshold import fails, check the following log files:

Linux: \$NnmDataDir/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Note: -u <username> -p <password> are optional parameters.

Configuring QoS Thresholds

NNM iSPI Performance for QA QoS thresholds enables you to track the health and performance of the QoS interfaces and nodes in your network.

You can configure the thresholds based on the following QoS element types:

- QoS Class
- QoS Node Group
- QoS Parent Policy¹
- Independent QoS Policy (a policy that does not refer to any other policies)

You can establish thresholds for the probes associated with the QoS elements. You can configure these thresholds to create an incident whenever the network performance measurement assigned to the site breaches a threshold.

NNM iSPI Performance for QA performs the following actions if a threshold is breached:

- Sets the QoS element status to Major.
- Creates an incident for the violated threshold.
- Retains the threshold state as Nominal, or sets the threshold state to High or Low depending on the count-based, or time-based threshold configuration.

Note: The global manager receives the threshold states from the sites in the regional managers. The thresholds configured for the QoS elements of the global managers are not applicable for the sites of regional managers.

You can monitor the network performance and generate an incident based on the count-based threshold or time-based threshold configuration. However, you can only configure either a count-based or time-based threshold configuration for a combination of a QoS element and metric.

Threshold Configurations

Count-Based Threshold Configuration

You can generate an incident based on the count or number of consecutive times a metric violates the threshold value. You can define this count in the Threshold Configuration form.

Time-Based Threshold Configuration

Time-Based threshold configuration enables you to raise an alert when the threshold breached state persists for more than a specific time period. This is derived by specifying X as the duration of time in minutes when the metric is in a threshold breached state within Y number of minutes specified in the sliding window.

Example for Time-Based Threshold Configuration


Consider a scenario, where the polling interval is 5 minutes; High duration is 10 minutes; and High Duration Window is 60 minutes. In this scenario, an incident is generated whenever the High Duration exceeds 10 minutes within the 60 minute duration. NNM iSPI Performance for QA uses a sliding window wherein each time the High Duration (10 minutes) is reached, NNM iSPI Performance for QA drops the oldest polled value (first 5 minutes) and adds the most recent (between 60 to 65 minutes). This procedure continues and enables you to determine time-based threshold violation.

¹ A parent policy contains references to other policies, that are known as child policies. You can define thresholds only on the parent policies. However, NNM iSPI Performance for QA applies the parent policy threshold on the classes configured for the child policies too.




You can make utmost use of the Time-Based threshold violation by ensuring that the duration specified in the sliding window is greater than or equal to the polling interval.

Adding QoS Threshold Configuration

To add a new QoS threshold:


1. [Launch the QoS Threshold configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Threshold Configuration** > **QoS**. The QoS Threshold Configuration form opens.
2. In the Configured QoS Thresholds panel of the QoS Threshold Configuration form, click  **New**.
3. Specify the following to configure the threshold:



Field Name	Description
Name	<p>Specify the name you want to assign to the threshold.</p> <p>Threshold names are case sensitive. That is ThresholdA and thresholdA are considered two different thresholds.</p> <p>Threshold names must be unique. Also, it is recommended to use unique threshold names across the QoS elements in a GNM environment.</p> <p>Use only alphanumeric characters to define threshold names. Threshold names cannot contain special characters.</p>
Order	<p>Specify a numeric value. NNM iSPI Performance for QA checks for configuration settings in the order you define (lowest number first). NNM iSPI Performance for QA uses the first match found for each threshold. Provide a unique ordering number for each threshold.</p> <p>Thresholds with duplicate Order numbers are checked in random order.</p> <p>If a QoS interface or node applies to multiple criteria, NNM iSPI Performance for QA computes the breached threshold based on the ordering number (lower numbers are given higher priority) and generates an incident.</p> <p>For example, you configured threshold T1 based on the class called DefaultClass and T2 based on the node group Routers. The ordering number for T1 is 1 and T2 is 2.</p> <p>QoS interface Fa0/0 belongs to node group Routers and has DefaultClass configured on it. NNM iSPI Performance for QA considers threshold T1 to compute threshold violation and</p>

Field Name	Description
	incident generation.
Threshold Type	In the Threshold Type, select QoS Condition Based
Policy	Specify a QoS policy name on which you want to configure the threshold and click  to add the policy in the list. The QoS elements on which the selected policy is applied come under the threshold.
Class	Specify a QoS class name on which you want to configure the threshold and click  to add the class in the list. The QoS elements on which the selected class is applied come under the threshold.
Node Group	Specify a QoS node group on which you want to configure the threshold and click  to add the node group in the list. You must create a QoS node group in NNMi before configuring a QoS threshold on the node group.

You must specify at least one criterion for the threshold. That is, specify at least one policy, class, or node group for the threshold.

NNM iSPI Performance for QA enables you to use wildcard characters to define the policy, class, and node group criteria.

- On the Threshold Settings tab, click  **New** to configure the metrics for the threshold. For more information, see ["Adding QoS Threshold Settings " on the next page.](#)
- Use any one of the following options to complete creating the threshold:

Icon	Description
 Close	Closes the Add Threshold Configuration form without saving the threshold information you have entered.
 Save and Close	Saves the threshold information and closes the Threshold Configuration form.

- Click **Apply Threshold Now** in the QoS Threshold Configuration form to apply the threshold immediately (otherwise, the threshold is applied at the next discovery cycle).

To view the changes in the QoS Threshold Configuration form, click  **Refresh**.

- Check the following log file if you see an error:

Linux: \$NnmDataDir/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Adding QoS Threshold Settings

To configure the metrics for the threshold:

1. Specify the following to configure the threshold settings:


Field Name	Description
Type	Select the type of threshold violation. The valid types are Count-Based and Time-Based .
Metric	Select the metric for which you are configuring the threshold.

After you select the metric to configure the threshold, the list of fields relevant to the selected metric appear. You can specify the following values to configure the new threshold:

Field Name	Description
High Value	Enter the threshold value. This value indicates the maximum value above which the metric will be considered to have violated the Nominal range. For Packet Loss metric, enter the High Value in percentage.
High Value Rearm	<p>Enter the high value rearm for the threshold. For Packet Loss metric, enter the High Value Rearm in percentage.</p> <p>The High Value Rearm is used to indicate the end of the high threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value.</p> <p>The high value rearm must always be lower than the high value.</p> <p>Example</p> <p>For the Discarded Packets percentage, you must generate an incident when the percentage is 80 and clear the incident when the percentage comes down to 60.</p> <p>Set the following values for the threshold:</p> <ul style="list-style-type: none"> • High Value: 80 • High Value Rearm: 60 <p>This value enables you to be aware when a network performance problem starts to improve.</p>

The following field appears, if you selected the Type as Count-Based:

Field Name	Description
Trigger Count	Specify after how many consecutive threshold violations NNM iSPI Performance for QA must alert the operator by

Field Name	Description
	transitioning the threshold state to  High.



The following fields appear if you selected the Type as Time-Based:

Field Name	Description
High Duration	<p>Designate the minimum time within which the metric value must remain in the High range.</p> <p>For example if you specify this value to be 20 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 minutes.</p> <p>You define the high threshold value in the High Value field.</p> <p>The High Duration should be equal to or greater than the associated Polling Interval setting, because that is how often NNM iSPI Performance for QA provides a data point..</p>
High Duration Window	<p>Designate the window of time within which the High Duration criteria must be met.</p> <p>To enable this setting, the value must be:</p> <ul style="list-style-type: none"> • greater than 0 (zero) • the same as or greater than the High Duration value <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p> <p>For example, if you specify this value to be 30 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 out of 30 minutes.</p>

Select the following to generate an incident when the time-based threshold or count-based threshold value is violated:

Field Name	Description
Generate Incident	Select this option if you want NNM iSPI Performance for QA to generate an incident for count-based or time-based threshold violations. By default this option is selected.

2. Use any one of the following options to complete the task:

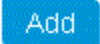
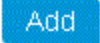
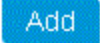
Icons	Description
 Close	Closes the Add Threshold Settings form without saving the threshold information you have entered.
 Save and Close	Saves the threshold information and closes the Threshold Settings form

- Continue creating the threshold in the Add QoS Threshold Configuration form.

Editing QoS Threshold Configuration

To edit an existing QoS threshold:



- Launch the QoS Threshold configuration form.
 - Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - In the **Configuration** workspace, select **Threshold Configuration** > **QoS**. The QoS Threshold Configuration form opens.
- You can edit the following settings:

Field Name	Description
Order	Specify a numeric value. NNM iSPI Performance for QA checks for configuration settings in the order you define (lowest number first). NNM iSPI Performance for QA uses the first match found for each threshold. Provide a unique ordering number for each threshold. Thresholds with duplicate Order numbers are checked in random order.
Policy	Specify a QoS policy name on which you want to configure the threshold and click  to add the policy in the list. The QoS elements on which the selected policy is applied come under the threshold.
Class	Specify a QoS class name on which you want to configure the threshold and click  to add the class in the list. The QoS elements on which the selected class is applied come under the threshold.
Node Group	Specify a QoS node group on which you want to configure the threshold and click  to add the node group in the list.

Make sure that you have specified at least one criterion for the threshold. That is, specify at least one policy, class, or node group for the threshold.

Note: If you create a new threshold configuration or modify the threshold configuration criteria (policy, class, or node group), NNM iSPI Performance for QA applies the changes in the next configuration polling cycle. However, NNM iSPI Performance for QA does not delete the incidents that are already generated for an existing threshold.

- Use any one of the following options to complete modifying the threshold:

Icons	Description
 Close	Closes the Add Threshold Configuration form without saving the threshold information you have entered.
 Save and Close	Saves the threshold information and closes the Threshold Configuration form

- Click **Apply Threshold Now** in the QoS Threshold Configuration form to apply the threshold immediately (otherwise, the threshold is applied at the next discovery cycle).

To view the changes in the QoS Threshold Configuration form, click  **Refresh**


Check the following log file if you see an error:

Linux: \$NnmDataDir/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Editing QoS Threshold Settings

To configure the metrics for the threshold:

- Make sure that you have specified the mandatory fields in the [editing QoS threshold configuration](#).
- Select the threshold settings, and Click  **Edit**
- Specify the following to configure the threshold settings:


Field Name	Description
Type	Select the type of threshold violation. The valid types are Count-Based and Time-Based .
Metric	Select the metric for which you are configuring the threshold. The metrics are populated based on the service.

After you select the metric to configure the threshold, the list of fields relevant to the selected metric appear. You can specify the following values to configure the new threshold:

Field Name	Description
High Value	Enter the threshold value. This value indicates the maximum

Field Name	Description
	value above which the metric will be considered to have violated the Nominal range. For Packet Loss metric, enter the High Value in percentage.
High Value Rearm	<p>Enter the high value rearm for the threshold. For Packet Loss metric, enter the High Value Rearm in percentage.</p> <p>The High Value Rearm is used to indicate the end of the high threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value.</p> <p>The high value rearm must always be lower than the high value.</p> <p>Example</p> <p>For the Discarded Packets percentage, you must generate an incident when the percentage is 90 and clear the incident when the percentage comes down to 60.</p> <p>Set the following values for the threshold:</p> <ul style="list-style-type: none"> • High Value: 90 • High Value Rearm: 60 <p>This value enables you to be aware when a network performance problem starts to improve.</p>

The following field appears, if you selected the Type as Count-Based:

Field Name	Description
Trigger Count	Specify after how many consecutive threshold violations NNM iSPI Performance for QA must alert the operator by transitioning the threshold state to  High.

The following fields appear if you selected the Type as Time-Based:



Field Name	Description
High Duration	<p>Designate the minimum time within which the metric value must remain in the High range.</p> <p>For example if you specify this value to be 20 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 minutes.</p> <p>You define the high threshold value in the High Value field.</p> <p>The High Duration should be equal to or greater than the associated Polling Interval setting, because that is how often</p>

Field Name	Description
	NNM iSPI Performance for QA provides a data point..
High Duration Window	<p>Designate the window of time within which the High Duration criteria must be met.</p> <p>To enable this setting, the value must be:</p> <ul style="list-style-type: none"> • greater than 0 (zero) • the same as or greater than the High Duration value <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p> <p>For example, if you specify this value to be 30 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 out of 30 minutes.</p>

Select the following to generate an incident when the time-based threshold or count-based threshold value is violated:

Field Name	Description
Generate Incident	Select this option if you want NNM iSPI Performance for QA to generate an incident for count-based or time-based threshold violations. By default this option is selected.

4. Use any one of the following options to complete the task:

Icons	Description
 Close	Closes the Add Threshold Settings form without saving the threshold information you have entered.
 Save and Close	Saves the threshold information and closes the Threshold Settings form

5. Continue modifying the threshold in the Edit QoS Threshold Configuration form.




If you modify the threshold settings or update the monitored metrics, NNM iSPI Performance for QA applies the changes in the next polling cycle. For example, You have a threshold T1 that monitors the metric Dropped Packets. If you changed the configured threshold value for the metric from 5 to 10, NNM iSPI Performance for QA applies the changes in the next polling cycle.

However, NNM iSPI Performance for QA does not delete the incidents that are already generated for an existing threshold. For example, if an incident was already generated for threshold T1, NNM iSPI Performance for QA does not delete the incident when the metric value is changed from 5 to 10.

For a list of incidents generated for NNM iSPI Performance for QA threshold violations, see "[Threshold Incidents](#)" on page 136

Deleting QoS Thresholds


To delete an existing QoS threshold:

1. [Launch the QoS Threshold configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Threshold Configuration** > **QoS**. The QoS Threshold Configuration form opens.
2. Select a threshold in the **Threshold Settings** panel and click  **Delete**.
or
Click  **Delete All** to delete all QoS thresholds.
3. Click  **Refresh** in the Configured QoS Thresholds panel to view the changes.

However, NNM iSPI Performance for QA does not delete the incidents that are already generated for an existing threshold.

Importing QoS Thresholds

To import threshold configurations from an XML file:

1. [Launch the QoS Threshold configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Threshold Configuration** > **QoS**. The QoS Threshold Configuration form opens.
2. Click  **Import**.
3. In the user prompt dialog, enter the file name from where you want to import the QoS threshold configuration information.
You must enter the file name with full path information; for example, C:\temp\CBQoSthreshold_conf.xml
4. Click **OK** in the user prompt dialog.
If a threshold is already defined and displayed in the QoS Threshold Configuration panel, the import utility does not import the configuration information for this threshold from the XML file.

You can also import threshold configuration information using the following command line utility:

Linux: \$NnmInstallDir/bin/nmsgathresholdconfigutil.ovpl -u <username> -p <password> -import -type cbqos <filename>

Windows: %NnmInstallDir%\bin\nmsgathresholdconfigutil.ovpl -u <username> -p <password> -import -type cbqos <filename>

If the threshold import fails, check the following log files:

Linux: \$NnmDataDir/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Note: -u <username> -p <password> are optional parameters.

Exporting QoS Thresholds

To export the existing threshold configurations to an XML file:

1. [Launch the QoS Threshold configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Threshold Configuration** > **QoS**. The QoS Threshold Configuration form opens.

2. Click  **Export**.

3. Type the file name where you want to export the existing QoS threshold configuration in the user prompt dialog.

You must type the file name with full path information; for example, C:\temp\CbQoSthreshold_conf.xml

If you type the XML file name without entering the absolute path, by default the file gets saved in the following directory:

Linux: \$NnmDataDir/shared/qa/conf

Windows : %NnmDataDir%\shared\qa\conf

4. Click **OK** in the user prompt dialog.

You can also export the existing QoS threshold configuration using the following command line utility:

Linux: \$NnmInstallDir/bin/nmsqathresholdconfigutil.ovpl -u <username> -p <password> -export -type cbqos <filename>

Windows: %NnmInstallDir%\bin\nmsqathresholdconfigutil.ovpl -u <username> -p <password> -export -type cbqos <filename>

The threshold export utility does not export a threshold unless the threshold is associated with at least one site.

If the threshold export fails, check the following log files:

Linux: \$NnmDataDir/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Note: -u <username> -p <password> are optional parameters.

Supported QoS Threshold Configuration Metrics

You can configure threshold on the following metrics based on the selected device type:

QoS Metrics Metrics

Metric	Description
Pre Policy Bit Rate (kbps)	The bit rate of the traffic <i>per class</i> before applying the CBQoS policy, measured in kbps
Post Policy Bit Rate (kbps)	The bit rate of the traffic <i>per class</i> after applying the CBQoS policy, measured in kbps
Packet Drop (%)	<p>Percentage of the packets dropped <i>per class</i>.</p> <p>It is calculated using the following formula: $(\text{Total number of dropped packets} / \text{total number of packets transmitted per class}) * 100$</p>
Exceeded Packets (%)	<p>Percentage of the packets dropped <i>per class</i> due to exceeded policies</p> <p>It is calculated using the following formula: $(\text{Total number of packets dropped due to exceeded policies} / \text{total number of packets transmitted}) * 100$</p>
Violated Packets (%)	<p>Percentage of the packets dropped <i>per class</i> due to violated policies</p> <p>It is calculated using the following formula: $(\text{Total number of packets dropped due to violated policies} / \text{total number of packets transmitted}) * 100$</p>
Discarded Packets (%)	<p>Percentage of the packets dropped <i>per class</i> due to the queuing action</p> <p>It is calculated using the following formula: $(\text{Total number of packets dropped due to the queuing action} / \text{total number of packets transmitted}) * 100$</p>
Queue Utilization (%)	<p>Utilization rate for the queue</p> <p>It is calculated using the following formula: $(\text{Queue depth} / \text{Maximum queue depth}) * 100$</p>
Queue Bandwidth Utilization (%)	<p>Percentage of the bandwidth utilized <i>per class</i></p> <p>Available only when the bandwidth reservation per class is measured as one of the following values:</p> <ul style="list-style-type: none"> * As absolute value * As a percentage of the total bandwidth. It is calculated using the following formula: $(\text{PostPolicyBytes in kbps} / \text{Bandwidth configured in kbps}) * 100$
Dropped Shape Packets (%)	Percentage of packets dropped <i>per class</i> due to the shaping action

Metric	Description
	<p>It is calculated using the following formula: (Total number of packets dropped due to the shaping action / Number of packets transmitted for the selected class) * 100</p>
Delayed Shape Packets (%)	<p>Percentage of packets delayed <i>per class</i> due to the shaping action.</p> <p>It is calculated using the following formula: (Total number of packets delayed due to the shaping action/total number of packets transmitted)*100</p>
RED Packets Tail Drop (%)	<p>Percentage of packets dropped <i>per class</i> due to greater number of packets in the queue than the maximum threshold</p> <p>It is calculated using the following formula: (Total number of packets dropped by the RED algorithm / total number of packets transmitted)*100</p>
RED Packets Drop (%)	<p>Percentage of packets dropped <i>per class</i> due to the buffer overflow</p> <p>It is calculated using the following formula: (Total number of packets dropped by the RED algorithm / total number of packets transmitted)*100</p>
Marked DSCP Packets (%)	<p>Percentage of packets marked with IP DSCP bits <i>per class</i></p> <p>The class sets a configured DSCP value for the incoming IP packets.</p> <p>It is calculated using the following formula: (Packets with the IP DSCP bit set / total number of packets transmitted) * 100</p>
Marked IP Precedence Packets (%)	<p>Percentage of packets marked with IP Precedence <i>per class</i></p> <p>The class sets a configured Precedence value for the incoming IP packets.</p> <p>It is calculated using the following formula: (Packets with the IP precedence bit set / total number of packets transmitted) * 100</p>
Marked FRDE Packets (%)	<p>Percentage of packets marked with IP FRDE bits <i>per class</i></p> <p>The class sets a configured FRDE value for the incoming IP packets.</p> <p>It is calculated using the following formula: (Packets with the IP FRDE bit set / total number of packets transmitted) * 100</p>

Configuring QoS Thresholds for QA Groups

NNM iSPI Performance for QA enables you to track the health and performance of the QA groups, which you have configured and discovered. You can configure thresholds for both QA probes and QoS probes, and create incidents whenever the performance value assigned to the QA groups breaches the threshold.

NNM iSPI Performance for QA performs the following actions, if a threshold is breached:

- Sets the QA Groups (QA Probes or QoS) probes' status to major.
- Creates an incident for the violated threshold.
- Retains the threshold state as Nominal, or sets the threshold state to High or Low depending on the count-based, or time-based threshold configuration.

You can monitor the QA Groups entities for both QA Probes and QoS, and generate an incident based on the count-based threshold configuration or time-based threshold configuration.

Threshold Configuration

Count-Based Threshold Configuration

You can generate an incident based on the count or number of consecutive times a metric violates the threshold value. You can define this count in the Threshold Configuration form.

Time-Based Threshold Configuration

Time-Based threshold configuration enables you to raise an alert when the threshold breached state persists for more than a specific time period. This is derived by specifying X as the duration of time in minutes when the metric is in a threshold breached state within Y number of minutes specified in the sliding window.

Example for Time-Based Threshold Configuration

Consider a scenario, where the polling interval is 5 minutes; High duration is 10 minutes; and High Duration Window is 60 minutes. In this scenario, an incident is generated whenever the High Duration exceeds 10 minutes within the 60 minute duration. NNM iSPI Performance for QA uses a sliding window wherein each time the High Duration (10 minutes) is reached, NNM iSPI Performance for QA drops the oldest polled value (first 5 minutes) and adds the most recent (between 60 to 65 minutes). This procedure continues and enables you to determine time-based threshold violation.

You can make utmost use of the Time-Based threshold violation by ensuring that the duration specified in the sliding window is greater than or equal to the polling interval.

Baseline Settings Configuration

Baseline Deviation Settings Configuration

Apart from the time-based and count-based threshold configuration, you can also do [baseline monitoring](#) based on the baseline deviation setting configuration in NNM iSPI Performance for QA. You can do baseline deviation setting configuration for the selected probe, service, and metric. An incident is


generated and the baseline state transitions to Abnormal Range only if it meets all the criteria listed below:

- Exceeds the count or the number of standard deviation that is above the average value for the metric, or exceeds the count or the number of standard deviation that is below the average value for the metric. This count is specified in the Upper Baseline Limit Deviations or the Lower Baseline Limit Deviations in the baseline deviation settings configuration
- Exceeds the duration for which the upper or lower baseline deviation persists in the specified sliding window duration

Note: HP recommends that you have the probes with same frequency in a QA group for the Baseline Threshold feature to work effectively.


Adding QoS Threshold Configuration to QA Groups





To add threshold configuration to a QA Group:

1. [Launch the QoS Threshold configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Threshold Configuration** > **QoS**. The QoS Threshold Configuration form opens.
2. Click  **New** in the QoS Threshold Configuration form panel. The Add QoS threshold configuration form opens.
3. Specify the following to configure the threshold:

Field Name	Description
Name	The name of the Threshold setting. The name should be unique.
Order	Specify a numeric value. NNM iSPI Performance for QA checks the configuration settings in the order you define (lowest number first).
Threshold Type	In the Threshold Type, select QA Group Based .
QA Group condition	Lists the configured and discovered QoS QA Groups. You can select any one of the configured and discovered QoS QA Groups, from the drop down list to configure the threshold.


4. You can perform the following tasks in the **Threshold Settings** Tab:

Icon	Description
 New	Adds QA Group threshold settings.

Icon	Description
 Edit	Edits QA Group threshold settings.
 Delete	Deletes QA Group threshold settings.
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data.
 Delete All	Deletes all QA Group threshold settings.

Adding QoS Threshold Settings to QA Groups

To add a new threshold setting, do the following:


1. Specify all the mandatory fields when [adding QoS threshold configuration to QA groups](#).
2. Click  **New** in the **Threshold Settings** tab.
The Add Threshold settings form opens.
3. Specify the following to configure the threshold settings:

Field Name	Description
Type	Select the type of threshold violation. The valid types are Count-Based and Time-Based .
Metric	Select the metric for which you are configuring the threshold.

After you select the metric to configure the threshold, the list of fields relevant to the selected metric appear. You can specify the following values to configure the new threshold:

Field Name	Description
High Value	Enter the threshold value. This value indicates the maximum value above which the metric will be considered to have violated the Nominal range. For Packet Loss metric, enter the High Value in percentage.
High Value Rearm	Enter the high value rearm for the threshold. For Packet Loss metric, enter the High Value Rearm in percentage. The High Value Rearm is used to indicate the end of the high threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value. The high value rearm must always be lower than the high value. Example For the Discarded Packets percentage, you must generate an incident when

Field Name	Description
	<p>the percentage is 90 and clear the incident when the percentage comes down to 60.</p> <p>Set the following values for the threshold:</p> <ul style="list-style-type: none"> • High Value: 90 • High Value Rearm: 60 <p>This value enables you to be aware when a network performance problem starts to improve.</p>

Field Name	Description
Trigger Count	<p>Specify after how many consecutive threshold violations NNM iSPI Performance for QA must alert the operator by transitioning the threshold state to  High.</p>



The following fields appear if you selected the Type as Time-Based:

Field Name	Description
High Duration	<p>Designate the minimum time within which the metric value must remain in the High range.</p> <p>For example if you specify this value to be 20 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 minutes.</p> <p>You define the high threshold value in the High Value field.</p> <p>The High Duration should be equal to or greater than the associated Polling Interval setting, because that is how often NNM iSPI Performance for QA provides a data point..</p>
High Duration Window	<p>Designate the window of time within which the High Duration criteria must be met.</p> <p>To enable this setting, the value must be:</p> <ul style="list-style-type: none"> • greater than 0 (zero) • the same as or greater than the High Duration value <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p> <p>For example, if you specify this value to be 30 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 out of 30 minutes.</p>


- Select the following to generate an incident when the time-based threshold or count-based threshold value is violated:

Field Name	Description
Generate Incident	Select this option if you want NNM iSPI Performance for QA to generate an incident for count-based or time-based threshold violations. By default this option is selected.

- Use any one of the following options to complete the task:


Icons	Description
 Close	Closes the Add Threshold Configuration form without saving the threshold information you have entered.
 Save and Close	Saves the threshold information and closes the Threshold Configuration form.

After you configure the threshold settings, you can view the configured threshold details in the **Configured QoS Thresholds** tab.

- Continue creating the threshold in the Add QoS Threshold Configuration form.
- After you configure the threshold settings, Click  **Apply Threshold Now** in the QoS Threshold Configuration form, to apply the configured thresholds.

Editing QoS Threshold Configuration of QA Groups






To edit an existing threshold setting for a QA Group:

- Launch the [QoS Threshold configuration form](#).
 - Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - In the **Configuration** workspace, select **Threshold Configuration** > **QoS**. The QoS Threshold Configuration form opens.
- Select the configured threshold settings to modify, and click  **Edit** in the QoS Threshold Configuration form.
The Edit QoS threshold configuration form opens.
- Specify the following to configure the threshold:

Field Name	Description
Name	The name of the Threshold setting. The name should be unique.
Order	Specify a numeric value. NNM iSPI Performance for QA checks the configuration settings in the order you define (lowest number first).
Threshold Type	In the Threshold Type, select QA Groups Based .


Field Name	Description
QA Group condition	Lists the configured and discovered QoS QA Groups. You can select any one of the configured and discovered QoS QA Groups, from the drop down list.

You can perform the following tasks in the **Threshold Settings** Tab:

Icon	Description
 New	Adds QA Group threshold settings.
 Edit	Edits QA Group threshold settings.
 Delete	Deletes QA Group threshold settings.
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data.
 Delete All	Deletes all QA Group threshold settings.

Editing QoS Threshold Settings of QA Groups

To edit an existing threshold setting for a QA Group:

- Specify all the mandatory fields when [editing QoS threshold configuration of QA groups](#).
- Select the threshold setting to modify, and Click  **Edit** in the **Configured QoS Thresholds** panel.
The Edit QoS Threshold Settings form opens.
- Specify the following to configure the threshold settings:


Field Name	Description
Type	Select the type of threshold violation. The valid types are Count-Based and Time-Based .
Metric	Select the metric for which you are configuring the threshold. The metrics are populated based on the service. For information about the metrics for each service type, see " Supported Threshold Configuration Metrics " on page 299.

- After you select the metric to configure the threshold, the list of fields relevant to the selected metric appear. You can specify the following values to configure the new threshold:

Field Name	Description
High Value	Enter the threshold value. This value indicates the maximum value above which the metric will be considered to have violated the Nominal range. For Packet Loss metric, enter the High Value in percentage.

Field Name	Description
High Value Rearm	<p>Enter the high value rearm for the threshold. For Packet Loss metric, enter the High Value Rearm in percentage.</p> <p>The High Value Rearm is used to indicate the end of the high threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value.</p> <p>The high value rearm must always be lower than the high value.</p> <p>Example</p> <p>For the Discarded Packets percentage, you must generate an incident when the percentage is 90 and clear the incident when the percentage comes down to 60.</p> <p>Set the following values for the threshold:</p> <ul style="list-style-type: none"> • High Value: 90 • High Value Rearm: 60 <p>This value enables you to be aware when a network performance problem starts to improve.</p>

The following field appears, if you selected the Type as Count-Based:

Field Name	Description
Trigger Count	<p>Specify after how many consecutive threshold violations NNM iSPI Performance for QA must alert the operator by transitioning the threshold state to  High.</p>

The following fields appear if you selected the Type as Time-Based:



Field Name	Description
High Duration	<p>Designate the minimum time within which the metric value must remain in the High range.</p> <p>For example if you specify this value to be 20 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 minutes.</p> <p>You define the high threshold value in the High Value field.</p> <p>The High Duration should be equal to or greater than the associated Polling Interval setting, because that is how often NNM iSPI Performance for QA provides a data point..</p>
High Duration Window	<p>Designate the window of time within which the High Duration criteria must be met.</p> <p>To enable this setting, the value must be:</p>





Field Name	Description
	<ul style="list-style-type: none"> greater than 0 (zero) the same as or greater than the High Duration value <p>The NNM iSPI Performance for QA uses a sliding window. Each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polling interval and adds the most recent.</p> <p>For example, if you specify this value to be 30 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 out of 30 minutes.</p>

Select the following to generate an incident when the time-based threshold or count-based threshold value is violated:

Field Name	Description
Generate Incident	Select this option if you want NNM iSPI Performance for QA to generate an incident for count-based or time-based threshold violations. By default, this option is selected.


5. Use any one of the following options to complete the task:

Icons	Description
 Close	Closes the Edit Threshold Configuration form without saving the threshold information you have entered.
 Save and Close	Saves and applies the changes made.

6. Click  **Refresh** to view the changes in the **Configured QoS Thresholds** tab.
7. Click  **Save** or  **Save and Close** in the QoS Threshold Configuration form.
8. Click  **Apply Threshold Now** to enable the threshold.

Deleting QoS Threshold Settings of QA Groups

To delete an existing QoS threshold setting for a QA Group:

- Launch the [QoS Threshold configuration form](#).
 - Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - In the **Configuration** workspace, select **Threshold Configuration** > **QoS**. The QoS Threshold Configuration form opens.
- Select one or more configured threshold settings in the **Configured QoS Thresholds** tab, and click  **Delete**.

or


Click  **Delete All** to delete all QoS QA group threshold settings.

3. Click  **Refresh** in the QoS Threshold Configuration panel to view the changes.

However, NNM iSPI Performance for QA does not delete the incidents that are already generated for an existing threshold.

Importing QoS Thresholds of QA Groups

To import threshold configurations from an XML file:

1. [Launch the QoS Threshold configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Threshold Configuration** > **QoS**. The QoS Threshold Configuration form opens.
2. Click  **Import**.
3. In the user prompt dialog, enter the file name from where you want to import the QA Groups for QoS threshold configuration information.
You must enter the file name with full path information; for example,
C:\temp\QAGroupCBQoSthreshold_conf.xml
4. Click **OK** in the user prompt dialog.
If a threshold is already defined and displayed in the Configured QoS Thresholds panel, the import utility does not import the configuration information for this threshold from the XML file.

You can also import threshold configuration information using the following command line utility:

Linux: `$NnmInstallDir/bin/nmsqathresholdconfigutil.ovpl -u <username> -p <password> -import -type cbqos <filename>`

Windows: `%NnmInstallDir%\bin\nmsqathresholdconfigutil.ovpl -u <username> -p <password> -import -type cbqos <filename>`

If the threshold import fails, check the following log files:

Linux: `$NnmDataDir/log/qa/qa.log`


Windows: `%NnmDataDir%\log\qa\qa.log`

Note: -u <username> -p <password> are optional parameters.

Exporting QoS Thresholds of QA Groups

To export the existing QA Group threshold configurations:

1. [Launch the QoS Threshold configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The

- configuration console opens.
- b. In the **Configuration** workspace, select **Threshold Configuration > QoS**. The QoS Threshold Configuration form opens.
2. Click  **Export**.
 3. Type the file name where you want to export the existing QA Groups for QoS threshold configurations in the user prompt dialog.
You must type the file name with full path information; for example,
`C:\temp\QAGroupsCBQoSthreshold_conf.xml`
If you type the XML file name without entering the absolute path, by default the file gets saved in the following directory:
Linux: `$NnmDataDir/shared/qa/conf`
Windows : `%NnmDataDir%\shared\qa\conf`
 4. Click **OK** in the user prompt dialog.

You can also export the existing QA Groups for QoS threshold configurations using the following command line utility:

Linux: `$NnmInstallDir/bin/nmsqathresholdconfigutil.ovpl -u <username> -p <password> -export -type cbqos <filename>`

Windows: `NnmInstallDir%\bin\nmsqathresholdconfigutil.ovpl -u <username> -p <password> -export -type cbqos <filename>`

The threshold export utility does not export a threshold unless the threshold is associated with a QA Group.

If the threshold export fails, check the following log files:

Linux: `$NnmDataDir/log/qa/qa.log`

Windows: `%NnmDataDir%\log\qa\qa.log`

Note: `-u <username> -p <password>` are optional parameters.





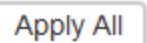




Configuring Ping Latency Pair Thresholds

Using ping latency pair thresholds, you can track the status of every ping pair you define in your environment. Using the NNM iSPI Performance for QA Configuration console, you can configure a threshold for a ping pair. The NNM iSPI Performance for QA generates incidents when a threshold violation is detected.

To configure the thresholds for ping pairs:

1. In the NNMi console, go to the Configuration workspace and click Quality Assurance Configuration. The NNM iSPI Performance for QA Configuration console opens.
2. In the NNM iSPI Performance for QA Configuration console, click **Ping Latency Thresholds**. The Ping Pair Threshold Configuration form opens.
3. You can perform the following tasks:



Tasks for Ping Pair Threshold Configuration

Task	Description
 Add	Launches the Ping Pair - Add Threshold Configuration form to add a new threshold.
 Edit	Selects an existing ping pair and launches the Ping Pair - Edit Threshold Configuration form to edit the threshold.
 Export	Exports threshold configurations.
 Import	Imports threshold configurations.
	Applies all the threshold configurations.
 Close	Closes the Threshold Configuration form without saving the current configuration.
 Refresh	Refreshes the list of thresholds.
 Delete	Deletes the selected ping pair thresholds.
 Delete All	Deletes all thresholds.

Adding Ping Latency Pair Thresholds



Note: Make sure QA groups are already created for ping pairs.

To add a new ping pair threshold:

1. Launch the Ping Pair - Add Threshold Configuration form.
2. In the Threshold Type section, specify the following details:
 - **Order:** Specify a numeric value. NNM iSPI Performance for QA checks the configuration settings in the order you define (lowest number first).
 - **QA Group:** Select a QA group of your choice. The threshold configuration is applied to all ping pairs that belong to the selected QA group.
3. Click  **Add** and use the [Ping Pair - Add Threshold Settings](#) form to add a threshold setting. You can add more than one threshold setting.
4. Click  **Save and Close**.



Adding Threshold Settings

To add a new ping pair threshold:

1. Launch the Ping Pair - Add Threshold Configuration form.
2. In the Threshold Type section, specify the following details:
 - **Type:** Select the metric type ([count-based](#) or [time-based](#)).
 - **Metric:** Select one of the following metrics:
 - Interface Utilization in Pair
 - RTT (ms)
 - Interface Utilization (%)
3. If you select *count-based*, specify the following details:
 - **High Value:** Type the threshold value. This value indicates the maximum value above which the metric will be considered to have violated the nominal range.
 - **High Value Rearm:** The High Value Rearm is used to indicate the end of the high threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value. Type a value lower than the High Value that you specified in the above step.
 - **Trigger Count:** Specify after how many consecutive threshold violations, the NNM iSPI Performance for QA must alert the operator by transitioning the threshold state to  High.
 - **Generate Incident:** Select this option if you want NNM iSPI Performance for QA to generate an incident. By default this option is selected.
4. If you select *time-based*, specify the following details:
 - **High Value:** Type the threshold value. This value indicates the maximum value above which the metric will be considered to have violated the nominal range.
 - **High Value Rearm:** The High Value Rearm is used to indicate the end of the high threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value. Type a value lower than the High Value that you specified in the above step.
 - **High Duration:** Type the minimum amount of time for which the ping pair must report high metric values.
 - **High Duration Window:** Define a window for the high duration value. This value must be greater than zero and can be same as the High Duration value.
 - **Generate Incident:** Select this option if you want NNM iSPI Performance for QA to generate an incident. By default this option is selected.
5. Click  **Save and Close**.

Adding Threshold Settings

To add a new ping pair threshold:

1. Launch the Ping Pair - Add Threshold Configuration form.
2. In the Threshold Type section, specify the following details:
 - **Type:** Select the metric type ([count-based](#) or [time-based](#)).
 - **Metric:** Select one of the following metrics:
 - Interface Utilization in Pair
 - RTT (ms)
 - Interface Utilization (%)
3. If you select *count-based*, specify the following details:
 - **High Value:** Type the threshold value. This value indicates the maximum value above which the metric will be considered to have violated the nominal range.
 - **High Value Rearm:** The High Value Rearm is used to indicate the end of the high threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value. Type a value lower than the High Value that you specified in the above step.
 - **Trigger Count:** Specify after how many consecutive threshold violations, the NNM iSPI Performance for QA must alert the operator by transitioning the threshold state to  High.
 - **Generate Incident:** Select this option if you want NNM iSPI Performance for QA to generate an incident. By default this option is selected.
4. If you select *time-based*, specify the following details:
 - **High Value:** Type the threshold value. This value indicates the maximum value above which the metric will be considered to have violated the nominal range.
 - **High Value Rearm:** The High Value Rearm is used to indicate the end of the high threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value. Type a value lower than the High Value that you specified in the above step.
 - **High Duration:** Type the minimum amount of time for which the ping pair must report high metric values.
 - **High Duration Window:** Define a window for the high duration value. This value must be greater than zero and can be same as the High Duration value.
 - **Generate Incident:** Select this option if you want NNM iSPI Performance for QA to generate an incident. By default this option is selected.
5. Click  **Save and Close.**

Count-Based Threshold Configuration

You can generate an incident based on the count or number of consecutive times a metric violates the threshold value. You can define this count in the Threshold Configuration form.

Time-Based Threshold Configuration

Time-Based threshold configuration enables you to raise an alert when the threshold breached state persists for more than a specific time period. This is derived by specifying X as the duration of time in minutes when the metric is in a threshold breached state within Y number of minutes specified in the sliding window.




Example for Time-Based Threshold Configuration

Consider a scenario, where the polling interval is 5 minutes; High duration is 10 minutes; and High Duration Window is 60 minutes. In this scenario, an incident is generated whenever the High Duration exceeds 10 minutes within the 60 minute duration. NNM iSPI Performance for QA uses a sliding window wherein each time the High Duration (10 minutes) is reached, NNM iSPI Performance for QA drops the oldest polled value (first 5 minutes) and adds the most recent (between 60 to 65 minutes). This procedure continues and enables you to determine time-based threshold violation.

You can make utmost use of the Time-Based threshold violation by ensuring that the duration specified in the sliding window is greater than or equal to the polling interval.


Edit an Existing Ping Pair Threshold

To edit an existing ping pair threshold:

1. Launch the Ping Pair - Edit Threshold Configuration form.
2. In the Threshold Type section, modify the following details:
 - **Order:** Specify a numeric value. NNM iSPI Performance for QA checks the configuration settings in the order you define (lowest number first).
 - **QA Group:** Select a QA group of your choice. The threshold configuration is applied to all ping pairs that belong to the selected QA group.
3. Click  **Add** and use the Ping Pair - Add Threshold Settings form to add a threshold setting . You can add more than one threshold setting. For more information about adding threshold settings, see "[Adding Threshold Settings](#)" on page 295
4. Click Delete  **Delete** to delete a threshold setting.
5. Click  **Save and Close**.

Exporting Ping Latency Pair Thresholds

To export the existing threshold configurations to an XML file:

1. [Launch the Ping Latency Pair Threshold Configuration form](#) .
2. Click  **Export**.
3. Type the file name where you want to export the existing threshold configuration in the user prompt dialog.

You must type the file name with full path information; for example, C:\temp\PL_threshold_conf.xml

If you type the XML file name without entering the absolute path, by default the file gets saved in the following directory:

Linux: \$NnmDataDir/shared/qa/conf

Windows : %NnmDataDir%\shared\qa\conf

4. Click **OK** in the user prompt dialog.

You can also export the existing threshold configuration using the following command line utility:

Linux: \$NnmInstallDir/bin/nmsqathresholdconfigutil.ovpl -u <username> -p <password> -export -type pingpair <filename>

Windows: %NnmInstallDir%\bin\nmsqathresholdconfigutil.ovpl -u <username> -p <password> -export -type pingpair <filename>

The threshold export utility does not export a threshold unless the threshold is associated with at least one site.

If the threshold export fails, check the following log files:


Linux: \$NnmDataDir/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Note: -u <username> -p <password> are optional parameters.

Importing the Ping Latency Pair Threshold Configurations

To import the existing threshold configurations from an XML file:

1. [Launch the Ping Latency Pair Threshold Configuration form](#) .
2. Click  **Import**.
3. In the user prompt dialog, enter the file name from where you want to import the threshold configuration information.

You must enter the file name with full path information; for example, C:\temp\PL_threshold_conf.xml

4. Click **OK** in the user prompt dialog.

If a threshold is already defined and displayed in the Site Wide Threshold Settings panel, the import utility does not import the configuration information for this threshold from the XML file.

You can also import threshold configuration information using the following command line utility:

Linux: \$NnmInstallDir/bin/nmsqathresholdconfigutil.ovpl -u <username> -p <password> -import -type pingpair <filename>

Windows: %NnmInstallDir%\bin\nmsqathresholdconfigutil.ovpl -u <username> -p <password> -import -type pingpair <filename>

If the threshold import fails, check the following log files:

Linux: \$NnmDataDir/log/qa/qa.log

Windows: %NnmDataDir%\log\qa\qa.log

Note: -u <username> -p <password> are optional parameters.

Supported Threshold Configuration Metrics

You can configure threshold on the following metrics based on the selected service type:

Note: Polling for two way packet loss metric is supported for all the probe types. However, threshold configuration for two way packet loss metric is supported only for ICMP Jitter and UDP probe types.

QA Threshold Metrics

Probe Service Type	Vendor			
	Cisco	Juniper	H3C	iRA Node
ICMP Echo	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS) 	RTT (microS)	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS) 	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS)
ICMP Jitter	Not supported	<ul style="list-style-type: none"> • RTT (microS) • Positive Jitter SD (microS) • Positive Jitter DS (microS) • Negative Jitter SD (microS) • Negative Jitter DS (microS) • Two way Jitter (microS) • Two way Packet Loss (%) 	Not supported	Not supported
UDP Echo	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS) 	RTT (microS)	RTT	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS)
UDP	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS) • Positive Jitter SD • Positive Jitter DS • Negative Jitter SD • Negative Jitter DS 	<ul style="list-style-type: none"> • RTT (microS) • Positive Jitter SD • Positive Jitter DS • Negative Jitter SD • Negative Jitter DS • Two way Jitter 	Not supported	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS)

QA Threshold Metrics, continued

Probe Service Type	Vendor			
	Cisco	Juniper	H3C	iRA Node
	<ul style="list-style-type: none"> • Packet Loss SD (%) • Packet Loss DS (%) • Two way Jitter • Two way Packet Loss (%) 	<ul style="list-style-type: none"> • Two way Packet Loss (%) 		
TCP Connect	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS) 	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS) 	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS) 	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS)
VoIP	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS) • Positive Jitter SD • Positive Jitter DS • Negative Jitter SD • Negative Jitter DS • Packet Loss SD (%) • Packet Loss DS (%) • Two way Jitter • Two way Packet Loss (%) • Mean Opinion Score (MOS) 	Not supported	Not supported	Not supported
Oracle	Not supported	Not supported	Not supported	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS)
HTTP	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS) 	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS) 	Not supported	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS)
HTTPS	Not supported	Not supported	Not supported	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS)
DNS	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS) 	Not supported	Not supported	Not supported
DHCP	<ul style="list-style-type: none"> • RTT (ms) • RTT (microS) 	Not supported	Not supported	Not supported

Note: For ICMP Jitter and UDP probe types (Juniper devices), the following metrics are collected only if one way hardware time stamp is enabled for a probe:

- Positive Jitter SD
- Positive Jitter DS
- Negative Jitter SD
- Negative Jitter DS

If one way hardware time stamp is changed for a probe between two discovery cycles, the metrics collected also changes accordingly. However, the change in the metrics collected takes effect only from the next discovery cycle. For example, a probe with one way hardware time stamp disabled does not collect the metrics listed above. However, if one way hardware time stamp is enabled later, the probe will collect all the metrics listed above, but this change takes effect only after the next discovery cycle.

Chapter 8: Configuring Global Network Management

The Global Network Management (GNM) configuration of the NNM iSPI Performance for QA provides distributed deployment capabilities in a network environment. An implementation of NNM iSPI Performance for QA in a GNM environment is very similar to an implementation of NNMi in a GNM environment. For more information about the GNM feature, see *Connecting Multiple NNMi management servers* in the *HP Network Node Manager i Software Online help*.

Before you implement the GNM configuration for the NNM iSPI Performance for QA, you must have implemented the GNM configuration for NNMi. The global manager and regional managers configured in NNMi **must be the same** in NNM iSPI Performance for QA. For example, a regional manager (RM) in NNMi cannot be a global manager (GM) in NNM iSPI Performance for QA.

It is not mandatory to configure the NNM iSPI Performance for QA in a GNM environment if NNMi is configured in the GNM environment. In such instances, the NNM iSPI Performance for QA can be installed on the NNMi GM, and the GM discovers the nodes that are hosting the QA probes as local nodes.

You must make sure that in a GNM environment all the NNMi management servers have time synchronization.


For more information about the GNM scenarios in NNM iSPI Performance for QA, see *Deploying NNM iSPI Performance for QA in a Global Network Management Environment* in the *NNM iSPI Performance for Quality Assurance Software Deployment Reference*.





Launching the Global Network Management Configuration Form

Perform the following steps to launch the Global Network Management Configuration form:

1. Log on to the global manager NNMi console using your user name and password.
You must have administrator privileges.
2. From the workspace navigation panel, select **Configuration** workspace.
3. Select **Quality Assurance Configuration Console**.
The console opens.
4. In the **Configuration** workspace, select **Global Network Management**.
The Global Network Management configuration form opens.

You can perform the following tasks from the Global Network Management toolbar:

Icon	Description
 New	Creates Regional Managers.


 Open	Edits Regional Managers.
 Delete	Deletes Regional Managers.
 Refresh	Refreshes and displays the last saved regional manager configuration details.
 Close	Closes the GNM form without saving the current configuration.

You can view the following details if you have configured a regional manager:

Field Name	Description
Name	The connection name for the regional NNMi management server.
Description	A description for the regional manager connection.
UUID	The Universally Unique Identifier of the regional manager.
Connection State	The Connection status can be one of the following: <ul style="list-style-type: none"> • Not Established • Connected



Creating Regional Managers

To create a new regional manager:





1. [Launch the Global Network Management Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Global Network Management**. The Global Network Management configuration form opens.
2. Click  **New**. The Regional Manager Configuration form opens.
3. Enter values for the following:

Field Name	Description
Name	Type the connection name for the regional NNMi management server. Ensure that the regional manager connection name is the same as the connection name specified for NNMi.
Description	Optional. Type a description for the regional manager.

4. Select one of the following options:

Option	Description
 Close	Closes the Create New Regional Manager Configuration form without saving the information you entered.
 Save	Saves the regional manager configuration.


5. You can perform the following tasks when you click the **Connections** tab:

Icon	Description
 New	Adds Regional Manager Connections.
 Open	Edits Regional Manager Connections.
 Delete	Deletes Regional Manager Connections.
 Refresh	Refreshes and displays the last saved regional manager connection.

Editing Regional Managers

You can modify an existing regional manager and regional manager connections.

To modify a regional manager, do the following:



1. [Launch the Global Network Management Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Global Network Management**. The Global Network Management configuration form opens.
2. Select the regional manager you want to modify and click  **Open**.

The Modify Regional Manager Configuration form opens.





3. You can modify the following information:

Field Name	Description
Name	Type the connection name for the regional NNMi management server. Make sure that the regional manager connection name is same as the connection name specified for NNMi.
Description	Optional. Type a description for the regional manager connection.

4. Select one of the following options:

Option	Description
 Close	Closes the Add Regional Manager Connection form without saving the information you have entered.
 Save	Saves the regional manager connection information.



5. You can perform the following tasks when you click the **Connections** tab:

Icon	Description
 New	Adds Regional Manager Connections.
 Open	Edits Regional Manager Connections.
 Delete	Deletes Regional Manager Connections.
 Refresh	Refreshes and displays the last saved regional manager connection.

Deleting Regional Managers


If you delete a regional manager configuration, all the objects associated with the regional manager such as sites are also deleted.

To delete a regional manager configuration, do the following:

1. [Launch the Global Network Management Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Global Network Management**. The Global Network Management configuration form opens.
2. Select the regional manager you want to delete and click  **Delete**.
3. Click  **Refresh** to view the changes.

Adding Regional Manager Connections

1. [Launch the Global Network Management Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Global Network Management**. The Global Network Management configuration form opens.

2. Ensure that you enter the name in the [Regional Manager Configuration](#) form.
3. Click  **New** in the **Connections** panel of the Regional Manager Configuration form.

The Add Regional Manager Connection form opens.

4. Enter values for the following:

- a. **Hostname**

The Fully Qualified Domain Name (FQDN) of the NNMi management server that must be connected as the regional manager.

- b. **Use Encryption**

If you select this option, NNM iSPI Performance for QA uses the Hypertext Transfer Protocol Secure (HTTPS) to connect to the regional NNMi management server.

If you do not select this option, NNM iSPI Performance for QA uses the Hypertext Transfer Protocol (HTTP) to connect to the regional NNMi management server.

If you have selected HTTPS option in NNMi management server, you must select the Use Encryption option. However, if you have selected the HTTP option in NNMi management server, you must clear the Use Encryption option.

- c. **HTTP(S) Port**

If you have selected the Use Encryption (previous field), enter the HTTPS port number for NNM iSPI Performance for QA. The default HTTPS port number for NNM iSPI Performance for QA is 54043.

If you have not selected the Use Encryption (previous field), enter the HTTP port number for NNM iSPI Performance for QA. The default HTTP port number for NNM iSPI Performance for QA is 54040.

- d. **User Name**

Type a valid user name for the regional NNMi management server.



- e. **User Password**

Type the password for the User Name.

- f. **Ordering**

Provide a unique connection ordering number for each regional manager configuration. NNM iSPI Performance for QA checks for configuration settings in the order you define (from lowest number to highest number). NNM iSPI Performance for QA uses the first match found for each address.

5. Perform one of the following actions:

Icon	Description
 Close	Closes the Add Regional Manager Connection form without saving the information you have entered.
 Save	Saves the regional manager connection information.

Modifying Regional Manager Connections

1. [Launch the Global Network Management Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Global Network Management**. The Global Network Management configuration form opens.
2. Select the regional manager connection you want to modify.

3. Click  **Open**.

The Modify Regional Manager Connection Configuration form opens.

4. Modify the values for the following:
 - a. **Hostname**

The Fully Qualified Domain Name (FQDN) of the NNMi management server that should be connected as the regional manager.
 - b. **Use Encryption**

If you select this option, NNM iSPI Performance for QA uses the Hypertext Transfer Protocol Secure (HTTPS) to connect to the regional NNMi management server.

If you do not select this option, NNM iSPI Performance for QA uses the Hypertext Transfer Protocol (HTTP) to connect to the regional NNMi management server.

If you have selected HTTPS option in NNMi management server, you must select the Use Encryption option. However, if you have selected the HTTP option in NNMi management server, you must clear the Use Encryption option.
 - c. **HTTP(S) Port**



If you have selected the Use Encryption (previous field), enter the HTTPS port number for NNM iSPI Performance for QA. The default HTTPS port number for NNM iSPI Performance for QA is 54043.

If you have not selected the Use Encryption (previous field), enter the HTTP port number for NNM iSPI Performance for QA. The default HTTP port number for NNM iSPI Performance for QA is 54040.
 - d. **User Name**

Type a valid user name of the regional NNMi management server.
 - e. **User Password**

Type the password for User Name.
 - f. **Ordering**




Type a numeric value. NNM iSPI Performance for QA checks for configuration settings in the order you define (from lowest number to highest number). NNM iSPI Performance for QA uses the first match found for each address. Provide a unique connection ordering number for each regional manager configuration.
5. Perform one of the following actions:

Icon	Description
 Close	Closes the Modify Regional Manager Connection form without saving the information you have entered.
 Save	Saves the regional manager connection information.

Deleting Regional Manager Connections

If you delete a regional manager configuration, all the objects associated with the regional manager are also deleted.

To delete a regional manager connection, do the following:

1. [Launch the Global Network Management Configuration form.](#)
 - a. Select **Configuration** workspace > **Quality Assurance Configuration Console**. The configuration console opens.
 - b. In the **Configuration** workspace, select **Global Network Management**. The Global Network Management configuration form opens.
2. Select the regional manager you want to delete and click  **Open**. The Modify Regional Manager Configuration form opens.
3. Select the regional manager connection in the Connections panel, and click  **Delete**.
4. Click  **Refresh** in the Connections panel to view the changes.

Troubleshooting Global Network Management Configuration Error Messages

The error log files are available in the following directory:

Linux: `./var/opt/OV/log/qa/qa.log`

Windows: `%NnmDataDir%\log\qa\qa.log`

[Regional manager name has to be specified before creating new connection](#)

Occurs when you try to add a new connection without entering the Regional Manager Name in the Regional Manager Configuration form.

Reason and Resolution

Before entering the regional manager connection details, you must enter the Regional Manager name in the Regional Manager Configuration form of NNM iSPI Performance for QA.

No connections configured

Occurs when you try to save the Add Regional Manager Connections form without entering the details

Reason and Resolution

You must enter the details in the Add Regional Manager Connections form before saving the details

An error occurred while modifying regional manager connection

Occurs when you try to save the modified regional manager connection details in the Regional Manager Configuration form

Reason and Resolution

Check any of the following log files:

Linux: `./var/opt/OV/log/qa/qa.log`

Windows: `%NnmDataDir%\log\qa\qa.log`

Invalid parameters for connection

Occurs when you try to save the regional manager connection details in the Regional Manager Configuration form

Reason and Resolution

Check the parameters entered in the Regional Manager connection form

Check any of the following log files:

Linux: `./var/opt/OV/log/qa/qa.log`

Windows: `%NnmDataDir%\log\qa\qa.log`

Connection parameters cannot be empty

Occurs when you try to save the regional manager connection details without entering the mandatory fields in the Add Regional Manager Connection form

Reason and Resolution

Enter the mandatory fields in the Add Regional Manager Connection form

Invalid Regional manager connection configuration information provided. NNMi cannot connect to: {1} {0}

Occurs when you try to save the Regional Manager Configuration form

Reason and Resolution

Check if you have entered the correct hostname, username, and password

Duplicate Order

Occurs when you enter an ordering number in the Add Regional Manager Connection form that is assigned to some other regional manager connection

Reason and Resolution

You must enter an ordering number that is not assigned to some other regional manager connection

Failed to add connection {0} for regional manager {1}

Occurs when you try to save the regional manager connection details in the Add Regional Manager Connection form.

Reason and Resolution

Check any of the following log files:

Linux: `./var/opt/OV/log/qa/qa.log`

Windows: `%NmDataDir%\log\qa\qa.log`

Valid Port Number ranges from 0 to 65535

Occurs when you try to save the regional manager connection details with invalid HTTP or HTTPS port number range

Reason and Resolution

You must enter the HTTP or HTTPS port number of NNM iSPI Performance for QA running on the Regional Manager . The valid range is between 0 to 65535, but you can use the port number range between 1024 to 65535 preferably.

Chapter 9: Configuring Polling

QoS Polling

You can set the polling interval for the QoS interfaces or actions that are not part of any QA group by specifying the value in the Polling Interval field in the QoS Polling tab.




Note: If the QoS interfaces or actions are part of a QA group and no polling frequency is specified for that group, it will take the default value, which is 5 minutes.

To configure the QoS polling interval:

1. In the NNMi console, go to the **Configuration** workspace and click **Quality Assurance Configuration Console**. The NNM iSPI Performance for QA Configuration console opens.
2. In the Configuration workspace, select **Polling Configuration**. The Polling Configuration form opens.
3. Select the **QoS Polling** tab.
4. Specify the polling interval in seconds in the **Polling Interval** field.

Note: You cannot use a polling interval that is less than 1 minute.

5. You can perform the following tasks using the Polling Configuration form:

Icon	Description
 Close	Closes without saving the polling interval details you specified.
 Save	Saves the polling interval details you specified.
 Save and Close	Saves the polling interval details you specified and closes the Polling Configuration form.

Note: It is recommended that you configure at least 300 seconds or a higher value for all QoS interfaces. To poll select interfaces with a higher frequency, use the QA Group-based polling.

Probe Polling

NNM iSPI Performance for QA enables you to override the probe-specific polling frequency by applying the global polling frequency for the QA probes.




Note: QA probe retains the probe-specific polling frequency only if its frequency is higher than the global polling frequency.

To override the probe-specific polling interval:

1. In the NNMi console, go to the **Configuration** workspace and click **Quality Assurance Configuration Console**. The NNM iSPI Performance for QA Configuration console opens.
2. In the Configuration workspace, select **Polling Configuration**. The Polling Configuration form opens.
3. Select the **Probes Polling** tab.
4. Specify the polling interval in seconds in the **Polling Frequency** field.

Note: You cannot use a polling interval that is less than 1 minute.

5. Select the **Override Probe Specific Polling Interval** check box to apply the global polling frequency for the QA probes.
6. You can perform the following tasks using the Polling Configuration form:

Icon	Description
 Close	Closes without saving the polling interval details you specified.
 Save	Saves the polling interval details you specified.
 Save and Close	Saves the polling interval details you specified and closes the Polling Configuration form.

Chapter 10: Managing QA Probes

Probe configuration form enables you to do the following:

- Create a probe
 - Identify the type of test or probe to run on the node. For example, the QA probe service type, and Virtual Routing and Forwarding (VRF) name etc.
 - Define the duration details to run the test or probe. For example, the frequency, the life time of the probe etc.
 - Define the payload details (optional). For example, the size of the packet, inter packet delay etc.
- Create a template for probe that can be reused and associated with any source and destination node
- Deploy the probe, or save the probe details to a file and deploy at a later point of time
- View the Real Time Line graph for the metrics of QA probes that are deployed successfully
- Reconfigure the probes if the deployment for the configured probes fail
- View the probe list and template list
- View the pre-configured probes and launch the real time line graph (if required)

Note: The NNM iSPI Performance for QA supports multi-tenant architecture. Multi-tenant architecture establishes a node to tenant association and determines the nodes that can be accessed by the user. However, you can configure the QA probes for a source node irrespective of whether you can access the destination node or not. A user with administrator privileges can configure probes.

Tasks	See
Configure Probes	"Using QA Probe Templates" on page 319
Deploy Probes	"Deploying QA Probes" on page 327
View Deployment Status	"Viewing QA Probe Deployment Status" on page 329
View Preconfigured Probes	"Viewing Pre-configured QA Probes Available" below
Create a Template	"Creating QA Probe Templates " on page 315
View a Probe List	"Viewing QA Probe List" on page 327
View a Template List	"Viewing Probe Template Inventory" on page 324

Viewing Pre-configured QA Probes Available

You can use the **Preconfigured Probes** tab to view the list of configured probes discovered and monitored by NNM iSPI Performance for QA. Also, you can launch the real time line graph for the probes.

To view the preconfigured probes list:

1. **Launch the Probe Configuration form.**

a. You can launch the Probe Configuration form from any one of the following ways:

To launch from the Nodes Inventory

- i. Click **Inventory** → **Nodes**.
- ii. From the Nodes inventory, select the nodes you want to configure the QA probes on.
- iii. Go to step b.

To launch from Network Overview

- i. Click **Topology Maps** → **Network Overview**.
- ii. From the Network Overview, select the nodes you want to configure the QA probes on.
- iii. Go to step b.

To launch from the Interfaces Inventory

- i. Click **Inventory** → **Interfaces**.
- ii. From the Interfaces inventory, select the interfaces you want to configure the QA probes on.
- iii. Go to step b.







To launch from the IP Addresses Inventory



- i. Click **Inventory** → **IP Addresses**.
- ii. From the IP Addresses inventory, select the required IP Addresses you want to configure the QA probes on.
- iii. Go to step b.


b. Select **Actions** → **Quality Assurance** → **Probe Configuration**. The Probe Configuration form opens.

2. **Select the Preconfigured Probes tab.**

You can view the following details:

Field Name	Description
Probe Status	The status that the QA probe returned. It can be one the following statuses: <ul style="list-style-type: none">•  Normal•  Warning•  Major•  Critical•  Unknown•  Disabled

Field Name	Description
	<ul style="list-style-type: none">  Not Polled  No Status <p>For more information on status, see "Supported QA Probe Statuses" on page 45.</p>
Probe Name	The name of the QA probe.
Owner	The owner of the QA probe.
Source Host name	The host name of the source node for which the QA probes are configured.
Destination IP Address	The destination IP address of the node.
Service	The service type of the QA probe. The valid service types are: <ul style="list-style-type: none"> DNS HTTP ICMP Echo TCP Connect UDP Echo UDP VoIP DHCP
VRF Name	The VRF name
ToS	The Type of Service specified for the probe.

3. To launch the Real Time Line Graph for the probes:
 - a. Select the probes and select the metric from the drop-down list.
 - b. Select  **Launch Real Time Graph**.
 The Real Time Line Graph opens in a new window.
 For more information about Real Time Line Graph, see ["Monitoring Using Graphs"](#) on page 124.

Creating QA Probe Templates

You can use the **Template Definition** tab to do the following tasks:

- Define a QA probe template that can be reused and associated with any source and destination node
- Edit or view an existing template
- View the probe definition template based on the author name
- Copy the template definition

To define a new probe template:

1. [Launch the Probe Configuration form.](#)

- a. You can launch the Probe Configuration form from any one of the following ways:

[To launch from the Nodes Inventory](#)

- i. Click **Inventory** → **Nodes**.
- ii. From the Nodes inventory, select the nodes you want to configure the QA probes on.
- iii. Go to step b.

[To launch from Network Overview](#)

- i. Click **Topology Maps** → **Network Overview**.
- ii. From the Network Overview, select the nodes you want to configure the QA probes on.
- iii. Go to step b.

[To launch from the Interfaces Inventory](#)


- i. Click **Inventory** → **Interfaces**.
- ii. From the Interfaces inventory, select the interfaces you want to configure the QA probes on.
- iii. Go to step b.

[To launch from the IP Addresses Inventory](#)

- i. Click **Inventory** → **IP Addresses**.
- ii. From the IP Addresses inventory, select the required IP Addresses you want to configure the QA probes on.
- iii. Go to step b.

- b. Select **Actions** → **Quality Assurance** → **Probe Configuration**. The Probe Configuration form opens.

2. Select the **Template Definition** tab.

3. Click  **New** in the toolbar below the **Template Definition** tab.

4. Select the author name to retrieve the template list based on the authors. NNM iSPI Performance for QA retrieves the author names defined in NNMi. The template list appears only if there is at least one existing template for the selected author.

5. Specify the Protocol Details and Duration Details for the QA probe:

Protocol Details

Field Name	Description
Template Name	<i>Mandatory information</i> Specify the name of the new probe template.
VRF Name	Specify the VRF name.
Service	<i>Mandatory information</i> Select one of the following service types: <ul style="list-style-type: none"> • DNS • HTTP • HTTPS • ICMP Echo • Oracle • TCP Connect • UDP • UDP Echo • VoIP • DHCP
ToS	Specify the Type of Service.

Duration Details

Field Name	Description
Frequency	<i>Mandatory information</i> The frequency at which the probe must run the tests. Click this field to enter the hour, minute, and seconds.
Life Time	Specify the life time of the probe. The default value is Forever. To override this value, click this field to enter the day, hour, and minute.
Time Out	Specify the maximum time period for the source node to wait for a response from the destination node. Click this field to enter the hour, minute, and seconds.

Based on the Service type that you selected, specify the following service details:

DNS Details

Specify the DNS address for the probe to resolve.

HTTP and HTTPS Details

Field Name	Description
Download Content	Specify whether to download the content of the destination web page or not. Set the value to True or False.
Proxy Server	Specify the HTTP proxy host name if you want to use a proxy server.
Proxy User Name	Specify the HTTP proxy user name.
HTTP URL	Specify the HTTP URL that the probe must use.
Proxy Port	Specify the HTTP proxy port number.
Proxy Password	Specify the HTTP proxy password.
Fail On Content Errors	Specify whether to fail the probe if the download of the destination web page content is incomplete or is complete, but with errors. Set the value to True or False. Specify a value here only if Download Content field is set to True.
HTTP Version	Specify the HTTP version.
HTTP Name Server	Specify the IP address of the server to resolve the host name of the destination web page.

ICMP Details

Field Name	Description
Packet Size	Specify the packet size.
Number of Packets	Specify the number of packets sent.
Inter Packet Delay (Milliseconds)	Specify the inter packet delay in milliseconds.

Oracle Details

Field Name	Description
User Name	<i>Mandatory information</i> Specify the Oracle database user name.
Database Name	<i>Mandatory information</i>

Field Name	Description
	Specify the name of the database running on the target Oracle server.
Password	<i>Mandatory information</i> Specify the Oracle database password.
SQL Query	Specify the SQL Query that the QA probe must run.

TCP Connect Details

Field Name	Description
Packet Size	Specify the packet size.
Number of Packets	Specify the number of packets sent.
Inter Packet Delay (Milliseconds)	Specify the inter packet delay in milliseconds.

UDP and UDP Echo Details

Specify the following information:

Field Name	Description
Packet Size	Specify the packet size.
Number of Packets	Specify the number of packets sent.
Inter Packet Delay (Milliseconds)	Specify the inter packet delay in milliseconds.

VoIP Details

Field Name	Description
Packet Size	Specify the packet size.
Number of Packets	Specify the number of packets sent.
Inter Packet Delay (Milliseconds)	Specify the inter packet delay in milliseconds.
Codec Type	<i>Mandatory information</i> Select the codec type.

6. Click  **Save** in the Template Definition toolbar.

After you save the template definition details, the details appear in the template list.

You can select a template in the template list and open, copy, or delete the template.

Using QA Probe Templates

You can use the **Probe Definition** tab to do the following tasks for the selected source and destination nodes:

- Create new probes
- Create probes using a pre-defined template
- Deploy the configured QA probes on the node
- Copy the probe definitions

To create a new probe definition:

1. [Launch the Probe Configuration form.](#)

- a. You can launch the Probe Configuration form from any one of the following ways:

[To launch from the Nodes Inventory](#)

- i. Click **Inventory** → **Nodes**.
- ii. From the Nodes inventory, select the nodes you want to configure the QA probes on.
- iii. Go to step b.

[To launch from Network Overview](#)

- i. Click **Topology Maps** → **Network Overview**.
- ii. From the Network Overview, select the nodes you want to configure the QA probes on.
- iii. Go to step b.

[To launch from the Interfaces Inventory](#)

- i. Click **Inventory** → **Interfaces**.
- ii. From the Interfaces inventory, select the interfaces you want to configure the QA probes on.
- iii. Go to step b.

[To launch from the IP Addresses Inventory](#)

- i. Click **Inventory** → **IP Addresses**.
- ii. From the IP Addresses inventory, select the required IP Addresses you want to configure the QA probes on.
- iii. Go to step b.

- b. Select **Actions** → **Quality Assurance** → **Probe Configuration**. The Probe Configuration form opens.

2. Enter the Source Node and Destination Node details.

Source Node Details

Field Name	Description
Hostname	<i>Mandatory information</i> Specify the hostname of the source node for which you intend to configure the probes.
Tenant Name	Select an NNMI tenant from the list of tenants created in NNMI.

Field Name	Description
	NNMi provides a tenant named Default Tenant and assigns each newly discovered node to the Default Tenant and the Security Group attribute value configured for the Default Tenant. As an NNMi administrator, you can create new tenants and security groups. See <i>Configure Tenants</i> and <i>Configuring Security</i> in <i>HP Network Node Manager i Software Online Help: Help for Administrators</i> .
IP Address	Specify the IP address of the source node.
Port Number	Appears after you select the Service in the Probe Definition form. Specify the source port from which you intend to configure probes. However, this field does not appear if you select ICMP Echo service.
Write Community String	Specify the write community string to authenticate the source node. If you leave this field blank, NNM iSPI Performance for QA retrieves the SNMP Write Community String value from NNMi.

Destination Node Details

Field Name	Description
Hostname	Specify the hostname of the destination node for which you intend to configure the iRA probes.
IP Address	<i>Mandatory information</i> Specify the destination IP address for the iRA probe.
Port Number	Appears after you select the Service in the Probe Definition form. However, this field does not appear if you select ICMP Echo service. Specify the destination port for the probe.

- In the **Probe Definition** tab, specify the following details:

Protocol Details

Field Name	Description
Probe Name	<i>Mandatory information</i> Specify the name of the new probe.

Field Name	Description
VRF Name	Specify the VRF name.
Service	<p><i>Mandatory information</i></p> <p>Select any of the following service types:</p> <ul style="list-style-type: none"> • ICMP Echo • TCP Connect • UDP • UDP Echo • VoIP • HTTP • DNS • DHCP <p>After you select a service, the Port Number field appears for the Source Node Details and Destination Node Details sections. However, the Port Number field does not appear if you select ICMP Echo service.</p>
ToS	Specify the Type of Service.

4. Enter the following Duration Details:

Field Name	Description
Frequency	<p><i>Mandatory information</i></p> <p>The frequency at which the probe must run the tests. Click this field to enter the hour, minute, and seconds.</p>
Life Time	<p>Specify the life time of the probe. The default value is Forever. To override this value, click this field to enter the day, hour, and minute.</p>
Time Out	<p>Specify the maximum time period for the source node to wait for a response from the destination node. Click this field to enter the hour, minute, and seconds.</p>

Based on the Service type that you selected, specify the following service details:

ICMP Details

In the Packet Size field, specify the packet size.

TCP Connect Details

In the Packet Size field, specify the packet size.

UDP Details

Specify the following information:

Field Name	Description
Packet Size	Specify the packet size
Number of Packets	Specify the number of packets sent
Inter Packet Delay (Milliseconds)	Specify the inter packet delay in milliseconds

UDP Echo Details

In the Packet Size field, specify the packet size.

VoIP Details

Field Name	Description
Packet Size	Specify the packet size
Number of Packets	Specify the number of packets sent
Inter Packet Delay (Milliseconds)	Specify the inter packet delay in milliseconds
Codec Type	<i>Mandatory information</i> Select the codec type

HTTP Details

Field Name	Description
Download Content	Specify whether to download the content of the destination web page. Set the value to True or False.
Proxy Server	Specify the HTTP proxy hostname if you intend to use proxy server
Proxy User Name	Specify the HTTP proxy user name
HTTP URI	Specify the HTTP URL that the probe should use
Proxy Port	Specify the HTTP proxy port number





Field Name	Description
Proxy Password	Specify the HTTP proxy password
Fail On Content Errors	Specify whether to fail the probe if the download of the destination web page content is incomplete or is complete with errors. Set the value to True or False. You have to specify a value only if Download Content field is set to True.
HTTP Version	Specify the HTTP version
HTTP Name Server	Specify the IP address of the server to resolve the hostname of the destination web page

DNS Details

In the Address to resolve field, specify the address to be resolved.

Oracle Details

Field Name	Description
User Name	Specify the user name
Password	Specify the password
Database Name	Specify the database name
SQL Query	Specify the SQL Query

5. You can also create a probe using a pre-defined probe template by following the step below: Select the template in the **Select Template** list.
6. In the Probe Definition tab, click  **Deploy** to deploy a single probe. The Deploy operation performs the SNMP set operation on the selected source node.
7. To deploy multiple probes, follow these steps:
 - a. Click  **Add** to add the probes temporarily to the Probe List table.
 - b. Select the probes, and click  **Deploy**.
8. You can view the deployment status the QA probes that you configured in the [Deploy Status](#) tab.
9. Alternatively, you can save the probe configuration details to a file and deploy the probes at a later point of time. To save the probe configuration details to a file, you must click  **Save** in the Probe Configuration toolbar.

Viewing Probe Template Inventory

You can use the **Template List** tab to do the following tasks for the selected source and destination node:

- View the template definition in a new window
- Delete the selected template definition
- Select all the templates from the Template List

To access the template list:

1. [Launch the Probe Configuration form.](#)

- a. You can launch the Probe Configuration form from any one of the following ways:

[To launch from the Nodes Inventory](#)

- i. Click **Inventory** → **Nodes**.
- ii. From the Nodes inventory, select the nodes you want to configure the QA probes on.
- iii. Go to step b.

[To launch from Network Overview](#)

- i. Click **Topology Maps** → **Network Overview**.
- ii. From the Network Overview, select the nodes you want to configure the QA probes on.
- iii. Go to step b.

[To launch from the Interfaces Inventory](#)

- i. Click **Inventory** → **Interfaces**.
- ii. From the Interfaces inventory, select the interfaces you want to configure the QA probes on.
- iii. Go to step b.

[To launch from the IP Addresses Inventory](#)

- i. Click **Inventory** → **IP Addresses**.
- ii. From the IP Addresses inventory, select the required IP Addresses you want to configure the QA probes on.
- iii. Go to step b.

- b. Select **Actions** → **Quality Assurance** → **Probe Configuration**. The Probe Configuration form opens.

You can view two tabs below the Probe Configuration form; Probe List, and Template List





2. Select the **Template List** tab.

You can view the following details:

Field Name	Description
Template Name	The name of the QA probe template.
Service	The service type of the QA probe. It can be one of the following: <ul style="list-style-type: none">• UDP Echo• ICMP Echo

Field Name	Description
	<ul style="list-style-type: none"> • UDP • TCP Connect • VoIP • HTTP • DNS • DHCP
VRF Name	The name of the VRF.
ToS	The Type of Service specified in an IP packet header that indicates the service level required for the packet.
Frequency	The frequency at which the specific QA probe test must be repeated.
Life Time	The life time of the QA Probe.
Time Out	Maximum time the source node will wait for a response from the destination node before stopping the probes to run on the node.
Codec Type	The type of codec.
Packet Size	The size of each packet.
Number of Packets	The number of packets sent.
Inter Packet Delay (milliseconds)	The inter packet delay in milliseconds.


3. You can perform the following actions:

Icon	Description
 Open	Opens and allows to edit the selected template in the Template Definition form.
 Copy	Copies the selected template that appears in the Template Definition form.
 Delete	Deletes the selected template definition.
 Select All	Selects or deselects all the templates in the template list.



Deploying QA Probes



You can deploy the probes using the Probe Definition or Probe List form.

To deploy a probe using the **Probe Definition** form:

1. Enter the probe definition details. For more information see, "[Using QA Probe Templates](#)" on page 319.
2. Click  **Deploy** in the **Probe Definition** form.

To deploy the probes using the **Probe List** form:

1. Enter the probe definition details . For more information see, "[Using QA Probe Templates](#)" on page 319.
2. Click  **Add**. This adds the probes temporarily to the Probe List table.
3. Select the **Probe List** tab.
4. Select the probes you want to deploy.
5. Click  **Deploy** in the **Probe List** form.

Alternatively, you can click  **Open** in the Probe Configuration form. This opens a dialog box where you can specify to open a file with the probe configuration details. Select the **Probe List** tab, and select the probes to be deployed. Click  **Deploy** in the **Probe List** form.

Viewing QA Probe List

You can use the **Probe List** tab to do the following tasks for the selected source and destination node:

- View the configured probe definition in a new window
- Delete the selected probe definition
- Open the selected probe
- Deploy the selected probes on the node
- Enable to select all the probes in the Probe List

To access the probe list:

1. [Launch the Probe Configuration form.](#)
 - a. You can launch the Probe Configuration form from any one of the following ways:
[To launch from the Nodes Inventory](#)
 - i. Click **Inventory** → **Nodes**.
 - ii. From the Nodes inventory, select the nodes you want to configure the QA probes on.
 - iii. Go to step b.

To launch from Network Overview

- i. Click **Topology Maps** → **Network Overview**.
- ii. From the Network Overview, select the nodes you want to configure the QA probes on.
- iii. Go to step b.

To launch from the Interfaces Inventory

- i. Click **Inventory** → **Interfaces**.
- ii. From the Interfaces inventory, select the interfaces you want to configure the QA probes on.
- iii. Go to step b.

To launch from the IP Addresses Inventory

- i. Click **Inventory** → **IP Addresses**.
 - ii. From the IP Addresses inventory, select the required IP Addresses you want to configure the QA probes on.
 - iii. Go to step b.
- b. Select **Actions** → **Quality Assurance** → **Probe Configuration**. The Probe Configuration form opens.

You can view three tabs below the Probe Configuration form; Probe List, Template List, and Real Time Graph.






2. Select the **Probe List** tab.

You can view the following details:

Field Name	Description
Probe Name	The name of the QA probe.
Source IP Address	The source IP address of the node.
Destination IP Address	The destination IP address of the node.
Service	The service type of the QA probe can be any one of the following: <ul style="list-style-type: none">• UDP Echo• ICMP Echo• UDP• TCP Connect• VoIP• HTTP• DNS

Field Name	Description
	<ul style="list-style-type: none"> DHCP
ToS	The Type of Service specified in an IP packet header that indicates the service level required for the packet.
VRF Name	The name of the VRF.
Frequency	The frequency at which the specific QA probe test must be repeated.
Source Port	The source port from which the QA probes are configured.
Destination Port	The destination port until which the QA probes are configured.
Life Time	The life time of the QA Probe.
Time Out	Maximum time the source node will wait for a response from the destination node before stopping the probes to run on the node.
Codec Type	The type of codec.
Source Hostname	The host name of the source node for which the QA probes are configured.
Destination Hostname	The host name of the destination node for which the QA probes are configured.

3. You can find a list of options on the left-side below the Probe Configuration form. Select any one of the following options (if required):

Icon	Description
 Deploy	Deploys the selected configured probes on the selected node.
 Open	Opens and allows to edit the selected probe definition.
 Copy	Copies the selected probe that appears in the Probe Definition form.
 Delete	Deletes the selected probe definition.
 Select All	Selects or deselects all the probes in the probe list.

Viewing QA Probe Deployment Status

You can use the **Deploy Status** tab to do the following tasks:

- View the probe deployment status
- Launch the real time graph
- Select the probes to be reconfigured. You can only reconfigure probes whose Deploy Status is Failure.

To view the probe deploy status:

1. Select the **Deploy Status** tab in the Probe Configuration form.
2. On the left pane, you can view the following details:




Field Name	Description
Total Count	The total number of probes that you attempted to deploy irrespective of the status.
In Progress Count	The number of probes that are being deployed.
Success Count	The number of probes that were successfully deployed.
Failed Count	The number of probes that did not get deployed successfully.

3. On the right pane, you can view the following details:

Field Name	Description
Operational Status	The deployment status of the probe. The valid statuses are: <ul style="list-style-type: none"> • In-progress: Indicates the SNMP set operation is in progress • Success: Indicates the SNMP set operation is successful • Failure: Indicates the SNMP set operation is a failure
Source Hostname	The host name of the source node.
Probe Name	The name of the QA probe.
Owner	The owner of the QA probe.
Status Details	Displays a message after successful deployment of the probe, or indicates the reason for failure in the event of failure.

You can view the percentage of QA probes deployed irrespective of the deployment status in the status bar.

4. You can perform the following actions:

Icon	Description
 Edit	Allows to reconfigure the selected QA Probe details for which the deployment status is Failure.
 Launch Real Time Graph	Launches the real time line graph in a new window for the selected probes and metric.
 Refresh Status	Refreshes the details.

Maintaining QA Probes

The probes that are discovered can be enabled, disabled, or deleted using the Probe Maintenance form.

The Probe Maintenance form displays the following four tabs on the top of the user interface:

- [Probe List](#)
- [Enable Status](#)
- [Disable Status](#)
- [Delete Status](#)

Viewing the List of Probes

To view the list of probes:

1. [Launch the Probe Maintenance form.](#)
 - a. Click **Quality Assurance** workspace. The list of probes that are discovered in your network appears in the content pane.
 - b. Select a probe and click **Actions > Quality Assurance > Probe Maintenance**. The Probe Maintenance form opens.
 - c. Enter the following Node details:

Field Name	Description
Hostname	Select the host name of the source node.
Tenant Name	Specifies the NNMi tenant selected for the source node.
Write Community String	The write community string to use for authentication on the node.





2. Click on the **Probe List** tab.

You can view the following details:

Field Name	Description
Probe Status	The status of the QA probe.
Probe Name	The name of the QA probe.
Owner	The QA probe owner name.
Source Hostname	The hostname of the source node.
Destination IP Address	The destination IP address of the node.
Service	The service type of the QA probe. The valid service types are:

Field Name	Description
	<ul style="list-style-type: none"> • UDP Echo • ICMP Echo • UDP • TCP Connect • VoIP • DNS • HTTP • DHCP • Oracle
VRF Name	The name of the VRF.
ToS	The Type of Service specified in an IP packet header that indicates the service level required for the packet.

3. You can perform one of the following tasks from the Probe List tab:

Icon	Description
 Select All	Selects all the probes.
 Enable	Enables the selected probes and resumes the suspended operation.
 Disable	Disables the selected probes and suspends the operation.
 Delete	Deletes the selected probes from the device.

Viewing Probes with Enabled Status

You can use the **Enable Status** tab to do the following tasks for the selected source and destination node:

- View the probes that are enabled
- View the percentage of QA probes enabled in the status bar

To access the probes that are enabled:

1. [Launch the Probe Maintenance form.](#)
 - a. Click **Quality Assurance** workspace. The list of probes that are discovered in your network

appears in the content pane.

- b. Select a probe and click **Actions > Quality Assurance > Probe Maintenance**. The Probe Maintenance form opens.
- c. Enter the following Node details:

Field Name	Description
Hostname	Select the host name of the source node.
Tenant Name	Specifies the NNMi tenant selected for the source node.
Write Community String	The write community string to use for authentication on the node.

- 2. Click on the **Enable Status** tab.

You can view the following details:

Field Name	Description
Operational Status	The operational status of the QA probe.
Source Hostname	The hostname of the source node.
Probe Name	The name of the QA probe.
Owner	The QA probe owner name.
Status Details	The status of the QA probe.

You can view a status bar which displays the percentage of QA probes that are enabled.

Viewing Probes with Disabled Status

You can use the **Disable Status** tab to do the following tasks for the selected source and destination node:

- View the disable status
- View the percentage of QA probes disabled in the status bar

To access the probe list:

- 1. [Launch the Probe Maintenance form.](#)
 - a. Click **Quality Assurance** workspace. The list of probes that are discovered in your network appears in the content pane.
 - b. Select a probe and click **Actions > Quality Assurance > Probe Maintenance**. The Probe Maintenance form opens.
 - c. Enter the following Node details:

Field Name	Description
Hostname	Select the host name of the source node.

Field Name	Description
Tenant Name	Specifies the NNMI tenant selected for the source node.
Write Community String	The write community string to use for authentication on the node.

2. Click on the **Disable Status** tab.

You can view the following details:

Field Name	Description
Operational Status	The operational status of the QA probe.
Source Hostname	The hostname of the source node.
Probe Name	The name of the QA probe.
Owner	The QA probe owner name.
Status Details	The status of the QA probe.

You can view a status bar which displays the percentage of QA probes that are disabled.

Viewing Deleted Probes

You can use the **Delete Status** tab to do the following tasks for the selected source and destination node:

- View the deletion status
- View the percentage of QA probes deleted in the status bar

To access the probe list:

1. [Launch the Probe Maintenance form.](#)
 - a. Click **Quality Assurance** workspace. The list of probes that are discovered in your network appears in the content pane.
 - b. Select a probe and click **Actions > Quality Assurance > Probe Maintenance**. The Probe Maintenance form opens.
 - c. Enter the following Node details:

Field Name	Description
Hostname	Select the host name of the source node.
Tenant Name	Specifies the NNMI tenant selected for the source node.
Write Community String	The write community string to use for authentication on the node.

2. Click on the **Delete Status** tab.

You can view the following details:

Field Name	Description
Operational Status	The operational status of the node.
Source Hostname	The hostname of the source node.
Probe Name	The name of the QA probe.
Owner	The QA probe owner name.
Status Details	The status of the QA probe.

You can view a status bar which displays the percentage of QA probes that are deleted.

Managing QA Probes using Command Line Utility

You can use `nmsqaprobeconfig.ovpl` command to configure QA probes on a node for the following test types or services:

- ICMP Echo
- UDP
- UDP Echo
- TCP Connect
- HTTP (supported by Cisco, Juniper, and iRA)
- HTTPS (supported by iRA only)
- Oracle (supported by iRA only)
- DNS (supported by Cisco and iRA)
- DHCP (supported by Cisco and iRA)
- VoIP (supported by Cisco only)

Usage

For NNM iSPI Performance for QA

```
nmsqaprobeconfig.ovpl -u <username> -p <password> -c <write community string> -n
<hostname> -da <destination address> -tn <test name> -fr <test frequency> -tt icmp_
echo [-htn <Host Tenant Name> -da <destination address> -dp <destination port> -sa
<source address>] [-si <source interface name>] [-sp <source port>] [-vn <VRF
name>] [-tos <type of service>] [-lt <test life time in seconds>] [-to <test time
out in milliseconds>] [-ps <packet size>] [-pn <number of packets> [-pd <inter
packet delay in milliseconds>] [-ct <Cdec type>]
```

Option `-dp` is not valid for ICMP Echo.

Option `-ct` is valid only for VoIP tests.

For iRA

```
nmsqaprobeconfig.ovpl -u <username> -p <password> -c <write community string> -n
```

```
<hostname> -da <destination address> -tn <test name> -fr <test frequency> -tt icmp_
echo [-htn <Host Tenant Name> -da <destination address> -dp <destination port> -sa
<source address>] [-si <source interface name>] [-sp <source port>] [-lt <test life
time in seconds>] [-to <test time out in milliseconds>] [-ps <packet size>] [-pn
<number of packets>] [-pd <inter packet delay in milliseconds>]
```

Option -dp is not valid for ICMP Echo.

Parameters

- -u <username>: Type the user name.
- -p <password>: Type the password.
- -c <write community string>: Type the write community string to use for authentication on the remote node. If you leave this field blank, the value is retrieved from NNMi.
- -n <hostname>: Type the host name of the node. This is a required parameter.
- -tn <test name>: Type the name of the probe. This is a required parameter.
- -tt <test type>: Type the test type or service for which you want to configure QA probes. This is a required parameter.
 - The valid test types for NNM iSPI Performance for QA are icmp_echo, udp_echo, http, dns, dhcp, tcp_connect, udp, and voip.
 - The valid test types for iRA are icmp_echo, udp, udp_echo, tcp_connect, http, https, dns, dhcp, and oracle.
- -fr <test frequency>: Type the frequency at which the specific QA probe test must be repeated in seconds. This is a required parameter.
- -htn <host tenant name>: Type the tenant name for the host node. If you do not specify a tenant name, NNM iSPI Performance for QA uses NNMi default tenant.
- -sa <source address>: Type the source address of the probe in the node.
- -si <source interface name>: Type the source interface name of the probe in the node.
- -sp <source port>: Type the source port of the probe in the node.
- -da <destination address>: Type the destination address of the node for which you intend to configure QA probes. This is a required parameter.
- -dp <destination port>: Type the destination port. This is a required parameter if you have selected udp_echo, tcp_connect, udp, or voip service or test type.
- -vn <VRF name>: Type the name of the VRF.
This parameter is not valid for iRA probes.
- -tos <type of service>: Type the type of service.
This parameter is not valid for iRA probes.
- -lt <test life time>: Type the life time of the probe in seconds.
- -to <test time out>: Type the maximum time the source node will wait for a response from the destination node before stopping the request in milliseconds.
- -ps <packet size>: Type the size of the packet sent.
- -pn <number of packets>: Type the number of packets sent.

- `-pd <inter packet delay>`: Type the inter packet delay in milliseconds.
- `-ct <CdecType>`: Type the codec type you want to configure the QA probes. The valid codec types are `g711_u_law` or `g711_a_law` or `g729a`. This is a required parameter if you have selected the `voip` service.

The probes configured will be discovered in the next discovery cycle.

Note: `-u <username>` `-p <password>` are optional parameters.

Batch Upload of QA Probes

Use the following command to do a batch upload of a number of QA probes in NNM iSPI Performance for QA

```
nmsqaprobeconfig.ovpl -u <username> -p <password> -f <qa probe setup input file>
```

You can find the input file format `qaprobeconfig.tpl` in the following directory:

On Linux: `/var/opt/OV/shared/qa/conf`

On Windows: `%NnmDataDir%\shared\qa\conf`

This file gives you the format to enter the probe configuration details and upload the QA probes.

While you enter probe configuration details for a specific test type or service type in the QA probe setup input file, the user needs to enter only those parameters that are required and delete the other parameters. However, you must specify the test name in the QA probe setup input file for all the test type or service type.

Note: `-u <username>` `-p <password>` are optional parameters.

Managing iRA QA Probes

You can do the following to manage the iRA probes:

- Define an iRA probe template that can be reused and associated with any source and destination node.
- View the status of the deployed iRA probe.
- View the list of configured iRA probes discovered and monitored by NNM iSPI Performance for QA.
- Launch the real time graph.
- Reconfigure iRA probes that failed to deploy.

For more information, see the following topics:

- ["Creating iRA QA Probe Templates " below.](#)
- ["Viewing iRA QA Probe Deployment Status" on page 346](#)
- ["Viewing iRA Pre-configured QA Probes Available" on page 348.](#)

Creating iRA QA Probe Templates


Use the **Template Definition** tab to perform the following tasks:

- Define an iRA probe template that can be reused and associated with any source and destination node
- Edit or view an existing template
- View the probe definition template based on the author name
- Copy the template definition

To define a new probe template:

1. [Launch the Probe Maintenance form.](#)
 - a. Click **Quality Assurance** workspace. The list of probes that are discovered in your network appears in the content pane.
 - b. Select a probe and click **Actions > Quality Assurance > Probe Maintenance**. The Probe Maintenance form opens.
 - c. Enter the following Node details:

Field Name	Description
Hostname	Select the host name of the source node.
Tenant Name	Specifies the NNMi tenant selected for the source node.
Write Community String	The write community string to use for authentication on the node.

2. Select the **Template Definition** tab.
3. Click  **New** in the Template Definition toolbar.
4. Select the author name to retrieve the template list based on the authors. NNM iSPI Performance for QA retrieves the author names defined in NNMi. The template list appears only if there is at least one existing template for the selected author.
5. Specify the Protocol Details and Duration Details for the iRA probe:

[Protocol Details](#)

Field Name	Description
Template Name	<i>Mandatory information</i> Specify the name of the new probe template.
VRF Name	Specify the VRF name.
Service	<i>Mandatory information</i> Select any of the following service types: <ul style="list-style-type: none"> • DNS • HTTP • HTTPS • ICMP Echo

Field Name	Description
	<ul style="list-style-type: none"> • Oracle • TCP Connect • UDP • DHCP
ToS	Specify the Type of Service.

Duration Details

Field Name	Description
Frequency	<p><i>Mandatory information</i></p> <p>The frequency at which the probe must run the tests. Click this field to enter the hour, minute, and seconds.</p>
Life Time	<p>Specify the life time of the probe. The default value is Forever. To override this value, click this field to enter the day, hour, and minute.</p>
Time Out	<p>Specify the maximum time period for the source node to wait for a response from the destination node. Click this field to enter the hour, minute, and seconds.</p>

Based on the Service type that you selected, specify the following service details:

DNS Details

Specify the DNS address for the probe to resolve.

HTTP and HTTPS Details

Field Name	Description
Download Content	Specify whether to download the content of the destination web page or not. Set the value to True or False.
Proxy Server	Specify the HTTP proxy host name if you want to use a proxy server.
Proxy User Name	Specify the HTTP proxy user name.
HTTP URL	Specify the HTTP URL that the probe must use.
Proxy Port	Specify the HTTP proxy port number.

Field Name	Description
Proxy Password	Specify the HTTP proxy password.
Fail On Content Errors	Specify whether to fail the probe if the download of the destination web page content is incomplete or is complete, but with errors. Set the value to True or False. Specify a value here only if Download Content field is set to True.
HTTP Version	Specify the HTTP version.
HTTP Name Server	Specify the IP address of the server to resolve the host name of the destination web page.

ICMP Details

Field Name	Description
Packet Size	Specify the packet size.
Number of Packets	Specify the number of packets sent.
Inter Packet Delay (Milliseconds)	Specify the inter packet delay in milliseconds.

Oracle Details

Field Name	Description
User Name	<i>Mandatory information</i> Specify the Oracle database user name.
Database Name	<i>Mandatory information</i> Specify the name of the database running on the target Oracle server.
Password	<i>Mandatory information</i> Specify the Oracle database password.
SQL Query	Specify the SQL Query that the QA probe must run.

TCP Connect Details

Field Name	Description
Packet Size	Specify the packet size.
Number of Packets	Specify the number of packets sent.
Inter Packet Delay (Milliseconds)	Specify the inter packet delay in milliseconds.

UDP and UDP Echo Details

Specify the following information:

Field Name	Description
Packet Size	Specify the packet size.
Number of Packets	Specify the number of packets sent.
Inter Packet Delay (Milliseconds)	Specify the inter packet delay in milliseconds.

VoIP Details

Field Name	Description
Packet Size	Specify the packet size.
Number of Packets	Specify the number of packets sent.
Inter Packet Delay (Milliseconds)	Specify the inter packet delay in milliseconds.
Codec Type	<i>Mandatory information</i> Select the codec type.

6. Click  **Save** in the Template Definition toolbar.

After you save the template definition details, the details appear in the template list.

You can select a template in the template list and open, copy, or delete the template.

Using iRA QA Probe Templates

Use the **Probe Definition** tab to do the following tasks for the selected source and destination node:

- Create a new iRA probe
- Create a probe using a pre-defined template
- Deploy the configured iRA probes on the node
- Copy the probe definition

To create a new probe definition:

1. [Launch the Probe Configuration form.](#)

a. You can launch the Probe Configuration form from any one of the following ways:

[To launch from the Nodes Inventory](#)

- Click **Inventory** → **Nodes**.
- From the Nodes inventory, select the nodes you want to configure the QA probes on.
- Go to step b.

To launch from Network Overview

- i. Click **Topology Maps** → **Network Overview**.
- ii. From the Network Overview, select the nodes you want to configure the QA probes on.
- iii. Go to step b.

To launch from the Interfaces Inventory

- i. Click **Inventory** → **Interfaces**.
- ii. From the Interfaces inventory, select the interfaces you want to configure the QA probes on.
- iii. Go to step b.

To launch from the IP Addresses Inventory

- i. Click **Inventory** → **IP Addresses**.
- ii. From the IP Addresses inventory, select the required IP Addresses you want to configure the QA probes on.
- iii. Go to step b.

- b. Select **Actions** → **Quality Assurance** → **Probe Configuration**. The Probe Configuration form opens.

2. Specify the Source Node and Destination Node details.

Source Node Details

Field Name	Description
Hostname	<i>Mandatory information</i> Specify the hostname of the source node for which you intend to configure the probes.
Tenant Name	Select an NNMi tenant from the list of tenants created in NNMi. NNMi provides a tenant named Default Tenant and assigns each newly discovered node to the Default Tenant and the Security Group attribute value configured for the Default Tenant. As an NNMi administrator, you can create new tenants and security groups. See <i>Configure Tenants</i> and <i>Configuring Security</i> in <i>HP Network Node Manager i Software Online Help: Help for Administrators</i> .
IP Address	Specify the IP address of the source node.
Port Number	<i>Mandatory information</i> Appears after you select the Service in the Probe Definition form. Specify the source port from which you intend to configure probes.

Field Name	Description
	However, this field does not appear if you select ICMP Echo service.
Write Community String	Specify the write community string to authenticate the source node. If you leave this field blank, NNM iSPI Performance for QA retrieves the SNMP Write Community String value from NNMi.

Destination Node Details

Field Name	Description
Hostname	Specify the hostname of the destination node for which you intend to configure the iRA probes.
IP Address	<i>Mandatory information</i> Specify the destination IP address for the iRA probe.
Port Number	Appears after you select the Service in the Probe Definition form. However, this field does not appear if you select ICMP Echo service. Specify the destination port for the probe.

3. In the **Probe Definition** tab, specify the following details:

Protocol Details

Field Name	Description
Probe Name	<i>Mandatory Information</i> Specify the name of the new probe
VRF Name	Specify the VRF name
Service	Select any one of the following service types: <ul style="list-style-type: none"> • DNS • HTTP • HTTPS • ICMP Echo • Oracle • TCP Connect

Field Name	Description
	<ul style="list-style-type: none"> • UDP • DHCP <p>After you select a service, the Port Number field appears for the Source Node Details and Destination Node Details sections.</p> <p>However, the Port Number field does not appear if you select ICMP Echo and DNS service.</p>
ToS	Specify the Type of Service

Duration Details

Field Name	Description
Frequency	<p><i>Mandatory information</i></p> <p>The frequency at which the probe must run the tests.</p> <p>Click this field to enter the hour, minute, and seconds.</p>
Life Time	<p>Specify the life time of the probe.</p> <p>The default value is Forever.</p> <p>To override this value, click this field to enter the day, hour, and minute.</p>
Time Out	<p>Specify the maximum time period for the source node to wait for a response from the destination node.</p> <p>Click this field to enter the hour, minute, and seconds.</p>

Service Details

Based on the Service type that you selected, specify the following service details:

DNS Details

Specify the DNS address for the probe to resolve.

HTTP and HTTPS Details

Field Name	Description
Download Content	Specify whether to download the content of the destination web page or not. Set the value to True or False.
Proxy Server	Specify the HTTP proxy host name if you want to use a proxy server.
Proxy User Name	Specify the HTTP proxy user name.

Field Name	Description
HTTP URL	Specify the HTTP URL that the probe must use.
Proxy Port	Specify the HTTP proxy port number.
Proxy Password	Specify the HTTP proxy password.
Fail On Content Errors	Specify whether to fail the probe if the download of the destination web page content is incomplete or is complete, but with errors. Set the value to True or False. Specify a value here only if Download Content field is set to True.
HTTP Version	Specify the HTTP version.
HTTP Name Server	Specify the IP address of the server to resolve the host name of the destination web page.

ICMP Details

Field Name	Description
Packet Size	Specify the packet size.
Number of Packets	Specify the number of packets sent.
Inter Packet Delay (Milliseconds)	Specify the inter packet delay in milliseconds.

Oracle Details

Field Name	Description
User Name	<i>Mandatory information</i> Specify the Oracle database user name.
Database Name	<i>Mandatory information</i> Specify the name of the database running on the target Oracle server.
Password	<i>Mandatory information</i> Specify the Oracle database password.
SQL Query	Specify the SQL Query that the QA probe must run.

TCP Connect Details

Field Name	Description
Packet Size	Specify the packet size.

Field Name	Description
Number of Packets	Specify the number of packets sent.
Inter Packet Delay (Milliseconds)	Specify the inter packet delay in milliseconds.





UDP and UDP Echo Details

Specify the following information:

Field Name	Description
Packet Size	Specify the packet size.
Number of Packets	Specify the number of packets sent.
Inter Packet Delay (Milliseconds)	Specify the inter packet delay in milliseconds.

VoIP Details

Field Name	Description
Packet Size	Specify the packet size.
Number of Packets	Specify the number of packets sent.
Inter Packet Delay (Milliseconds)	Specify the inter packet delay in milliseconds.
Codec Type	<i>Mandatory information</i> Select the codec type.

4. You can also create a probe using a pre-defined probe template by following the step below: Select the template in the **Select Template** list.
5. In the Probe Definition tab, click  **Deploy** to deploy a single probe. The Deploy operation performs the SNMP set operation on the selected source node.
6. To deploy multiple probes, follow these steps:
 - a. Click  **Add** to add the probes temporarily to the Probe List table.
 - b. Select the probes, and click  **Deploy**.
7. You can view the deployment status the iRA probes that you configured in the [Deploy Status](#) tab.
8. Alternatively, you can save the probe configuration details to a file and deploy the probes at a later point of time. To save the probe configuration details to a file, you must click  **Save** in the Probe Configuration toolbar.

Viewing iRA QA Probe Deployment Status

You can use the **Deploy Status** tab to do the following tasks:

- View the probe deployment status
- Launch the real time graph
- Select the probes to be reconfigured. You can only reconfigure probes for which the deployment failed.

To view the probe deploy status:

1. Select the **Deploy Status** tab in the Probe Configuration form.
2. On the left pane, you can view the following details:



Field Name	Description
Total Count	The total number of probes that you attempted to deploy irrespective of the status.
In Progress Count	The number of probes that are being deployed.
Success Count	The number of probes that were successfully deployed.
Failed Count	The number of probes that did not get deployed successfully.

3. On the right pane, you can view the following details:

Field Name	Description
Operational Status	The deployment status of the probe. The valid statuses are: <ul style="list-style-type: none"> • In-progress: Indicates the SNMP set operation is in-progress • Success: Indicates the SNMP set operation is successful • Failure: Indicates the SNMP set operation is a failure
Source Host name	The host name of the source node.
Probe Name	The name of the probe.
Owner	The owner of the probe.
Status Details	Displays a message after successful deployment of the probe, or indicates the reason for failure in the event of failure

You can view the percentage of probes deployed irrespective of the deployment status in the status bar.

4. You can perform the following actions:

Icon	Description
 Edit	Enables you to reconfigure the details for the selected probe for which the deployment status is marked as Failure.
 Launch Real Time Graph	Launches the real time line graph in a new window for the selected probes and metric.

 Refresh	Refreshes the deployment status details.
---	--

Viewing iRA Pre-configured QA Probes Available

You can use the **Preconfigured Probes** tab to view the list of configured probes discovered and monitored by NNM iSPI Performance for QA. Also, you can launch the real time line graph for the probes.









To view the pre-configured probes list:

1. [Launch the Probe Maintenance form.](#)
 - a. Click **Quality Assurance** workspace. The list of probes that are discovered in your network appears in the content pane.
 - b. Select a probe and click **Actions > Quality Assurance > Probe Maintenance**. The Probe Maintenance form opens.
 - c. Enter the following Node details:


Field Name	Description
Hostname	Select the host name of the source node.
Tenant Name	Specifies the NNMi tenant selected for the source node.
Write Community String	The write community string to use for authentication on the node.

2. Select the **Preconfigured Probes** tab.

You can view the following details:

Field Name	Description
Probe Status	The probe status A probe may return any of the following status: <ul style="list-style-type: none"> •  Normal •  Warning •  Major •  Critical •  Unknown •  Disabled •  Not Polled •  No Status

Field Name	Description
	For more information on status, see "Supported QA Probe Statuses " on page 45 .
Probe Name	The name of the probe.
Owner	The owner of the probe.
Source Host name	The host name of the source node for which the probes are configured.
Destination IP Address	The destination IP address for the probe.
Service	The service type for the probe. The valid service types are: <ul style="list-style-type: none"> • DNS • HTTP • HTTPS • ICMP Echo • Oracle • TCP Connect • DHCP • UDP
VRF Name	The VRF name
ToS	The Type of Service specified for the probe.

3. To launch the Real Time Line Graph for the probes:
 - a. Select the probes and select the metric from the drop-down list.
 - b. Select  **Launch Real Time Graph**
The Real Time Line Graph opens in a new window
For more information about Real Time Line Graph, see ["Monitoring Using Graphs" on page 124](#).

Use Cases

Threshold Configuration

Module	NNM iSPI Performance for QA Threshold Configuration
Use Case Name	Configuring Site Based Thresholds for Two Way Jitter in VoIP Network
Use Case Author	HP Software

Summary

This use case provides a step by step process overview on creating threshold settings for two way jitter on a VoIP network.

Application

VoIP

Overview

To ensure end-to-end bandwidth with minimum jitter. If the two way jitter in the traffic flow is higher than 75, an incident will be generated.

Actors

- Network Administrator
- Capacity Planner
- Business Managers
- Network Designers
- Architects involved in deploying the network

Pre Condition

At least one site must be created before adding the threshold settings.

In this use case we have two sites, SiteA and SiteB. We need to monitor the two way jitter between these two sites.

Configure Threshold

- [Initialize the process](#)
- [Process](#)
- [Process termination](#)
- [Post conditions](#)
- [Exceptions](#)
- [GUIs referenced](#)

Assumptions

- User has administrative privileges to NNMi.
- User is using VoIP services to link between SiteA and SiteB.
- User wants to monitor the two way jitter(μsecs) between Site A and SiteB.
- Both SiteA and SiteB are created in the NNM iSPI Performance for QA Site Configuration form.

Initialization

1. Log on to NNMi console using a user name and password with administrator privileges.
2. From the workspace navigation panel, select **Configuration** workspace.
3. Select **Quality Assurance Configuration Console**.
The console opens.
4. In the **Configuration** workspace, select **Site Based Threshold**.
The Threshold Configuration form opens.

Threshold Configuration Process

This section describes all the typical interactions that take place between the actor and this use case.

Format: If the actor selects <selection>, the system will request the actor to enter information.

Perform the following steps to add a new threshold to a site:

1. Launch the Threshold Configuration form. See "[Threshold Configuration Process](#)" above.
2. Click *** New** in the Site Wide Threshold Settings panel.
The Add Threshold Configuration form opens.
3. Specify the following information in the Threshold Configuration panel:

Field Name	Description
Source Site	Select SiteA.
Destination site	Select SiteB.
Service Type	Select VoIP.

The new threshold you create is automatically assigned to the QA probes initiated from SiteA and run on the network elements in SiteB.

- Click  **New** in the Threshold Settings panel.

The Add Threshold Settings form opens.

- Specify the following values to configure the new threshold:

Field Name	Description
Type	Count-Based
Metric	Two Way Jitter(μsecs)
High Value	75
High Value Rearm	70
Trigger Count	2
Generate Incident	Select this option

- Click  **Save and Close**.




The Add Threshold Settings form closes.

- Click  **Save** in the Site Wide Threshold Configuration form.




- Click  **Refresh** in the Threshold Settings panel to view the threshold for the Two Way Jitter.

Process Termination


- Close the Add Threshold Configuration form by selecting any of the following options:

- Click  **Save and Close**.
- Click  **Save** and then click  **Close**.







- Close the Threshold Configuration form by selecting any of the following options:

- Click  **Save and Close**.
- Click  **Save** and then click  **Close**.

Exceptions

- You cannot create threshold settings if you do not have at least one site.
- If you do not select a destination site for the threshold settings, the settings will be applied to all the QA probes initiated from the source site.
- The new threshold will not be saved unless you click  **Save and Close** in the Add Threshold Settings form.

Post Conditions

- The threshold settings are applied to the poller immediately once you complete creating a threshold.
- The NNM iSPI Performance for QA applies the threshold for Two Way Jitter(μsecs) on all the QA probes run from SiteA and on SiteB.
- The NNM iSPI Performance for QA generates an incident if the Two Way Jitter(μsecs) crosses the high threshold value of 75 for two consecutive times.
- The Jitter column of the [QA Probes](#) view displays a  **High** state.
- The [Incident tab](#) in the QA Probes form displays a  **Critical** incident raised on the network element if an incident is raised.
- The [Threshold State](#) tab in the QA Probes form the threshold displays a  **High** state.
- The [Status tab](#) in the QA Probes form displays the network element status as  **Major**.
- The NNM iSPI Performance for QA clears the generated incident when the Two Way Jitter(μsecs) reaches the high value rearm of 70.
- The [Incident tab](#) in the QA Probes form reflects the change when an incident is cleared.
- The [Threshold State](#) tab in the QA Probes form the threshold displays a  **Nominal** state.
- The [Status tab](#) in the QA Probes form displays the network element status as  **Normal**.

You can view the threshold violated probes in the Threshold Exceptions probe view. In addition, you can view the report of the threshold violated probes view in the Network Performance server.

GUIs Referenced

- [Quality Assurance Threshold Configuration form](#)
- [Add Threshold Configuration form](#)
- [Add Threshold Settings form](#)

System Interface

NNM iSPI Performance for QA console

Glossary

C

child policy

The policy that the parent policy refers to.

D

delay

The time taken for a packet to travel from the sender network element to the receiver network element.

destination node

Usually the destination IRA node specifies the node, where you configured the Responder.

F

forwardable filters

The QA probes that are excluded and are not forwarded to the global manager based on the discovery filter.

H

High

The QA probe measure for the network element performance crossed the High threshold value.

I

In policy

In Policy defines the policy which is applied to the incoming traffic.

In Policy

In Policy defines the policy which is applied to the incoming traffic.

L

link status

Links are unidirectional for the QA probes originating from the source to the destination node. The color of the link is based on the threshold state of the probe for the selected service and metric.

Local QA Probes

Local QA probes are QA probes owned by the local sites.

Local Sites

Sites configured in the local NNMi management server are referred to as Local Sites. The local sites are owned by the Manager on which it is configured.

Low

The QA probe measure for the network element performance crossed the Low threshold value.

N

network element

Some examples of network elements are routers and switches.

network elements

Some examples of network elements are routers and switches.

Nominal

The QA probes measure for the network element performance was within healthy range, or no thresholds are being monitored.

Not Polled

Indicates that this network element is not polled intentionally.

O**ODBID**

ODBID is a custom attribute that the NNMi topology uses to integrate the NNMi topology with Business Service Management (BSM) software suite. The NNM iSPIs get this attribute from NNMi during the discovery and keep a reference. You can use ODBID as a report topology filter.

Out policy

Out Policy defines the policy which is applied to the outgoing traffic.

Out Policy

Out Policy defines the policy which is applied to the outgoing traffic.

P**parent policy**

The policy that contains references to other policy configurations. NNM iSPI Performance for QA displays only one hierarchical level for policies. For example, Policy1 contains references for Policy2 and NNM iSPI Performance for QA considers Policy2 as the child policy of Policy1. If Policy2 contains references to Policy3, the inventory views do not display Policy3 as a child of Policy1.

ping latency pair

A router-node pair used by the NNM iSPI Performance for QA to measure and monitor the connectivity between the router and the node. The router-node pair definition must be available in a configuration file provided by the NNM iSPI Performance for QA.

ping latency pairs

A router-node pair used by the NNM iSPI Performance for QA to measure and monitor the connectivity between the router and the node. The router-node pair definition must be available in a configuration file provided by the NNM iSPI Performance for QA.

probe

A probe is a test defined on a node to any destination node. You can manage those nodes in NNMi.

Probe

A probe is a pair of NNMi-managed nodes that support the IP SLA or RPM technology.

R**Remote QA Probes**

At Global server, the probes discovered and forwarded by regional servers are called as remote probes. You can manage threshold for these probes only at regional manager.

Remote Sites

Sites exported from the regional manager to the global manager are known as Remote Sites.

S**Site**

A logical organization of networking devices. In the scope of enterprise networks, a site can be a logical grouping of networking devices generally situated in similar geographic location. The location can include a floor, building or an entire branch office or several branch offices which connect to head quarters or another branch office via WAN/MAN. Each site is uniquely identified by its name. In case of the service provider networks the Virtual Routing and Forwarding (VRF) on a Provider Edge (PE) router or a

Customer Edge (CE) routers can be defined as a site.

site rules

Configuration associated to a site are called site rules. For example Node Group, Ordering, Test Name Pattern, etc are the site rules that are used to configure a site. The rules are prioritized inherently. The Node Group rule has the highest priority, the IP Address rule the second highest priority. Test Name Pattern rule has the third highest priority while the VRF Name rule has the lowest priority among these four rules. Note that none of these rules have any dependency to each other. In other words, while creating a site, you can specify all or any of the rules.

sites

A logical organization of networking devices. In the scope of enterprise networks, a site can be a logical grouping of networking devices generally situated in similar geographic location. The location can include a floor, building or an entire branch office or several branch offices which connect to head quarters or another branch office via WAN/MAN. Each site is uniquely identified by its name. In case of the service provider networks the Virtual Routing and Forwarding (VRF) on a Provider Edge (PE) router or a Customer Edge (CE) routers can be defined as a site.

source node

Usually the source IRA node specifies the node, where you configured the UDP Jitter probe.

status

The status and coloring scheme of the map component is derived based on the most severe operational status of all the QA probes originating from the source map component for the selected service, and metric. A map component can be a site in Site Map or node in Node Map.

T

TestUp

When both Administrative and Operational states are up.

U

Unavailable

Unable to compute the performance state of the network element, or the computed value is outside the valid range.

