HP Network Node Manager iSPI Performance for Quality Assurance Software

For the Windows ® and Linux operating systems

Software Version: 10.00

Online Help

Document Release Date: June 2014

Software Release Date: June 2014

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

Trademark Notices

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

DOM4J® is a registered trademark of MetaStuff, Ltd.

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

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

Acknowledgements

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

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

This product includes software developed by The Legion of The Bouncy Castle. (http://www.bouncycastle.org)

This product contains software developed by Trantor Standard Systems Inc. (http://www.trantor.ca)

Support

Visit the HP Software Support Online web site at: **http://www.hp.com/go/hpsoftwaresupport**

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

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

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

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

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

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

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**

Contents

Chapter 1: NNM iSPI Performance for QA 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.

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.

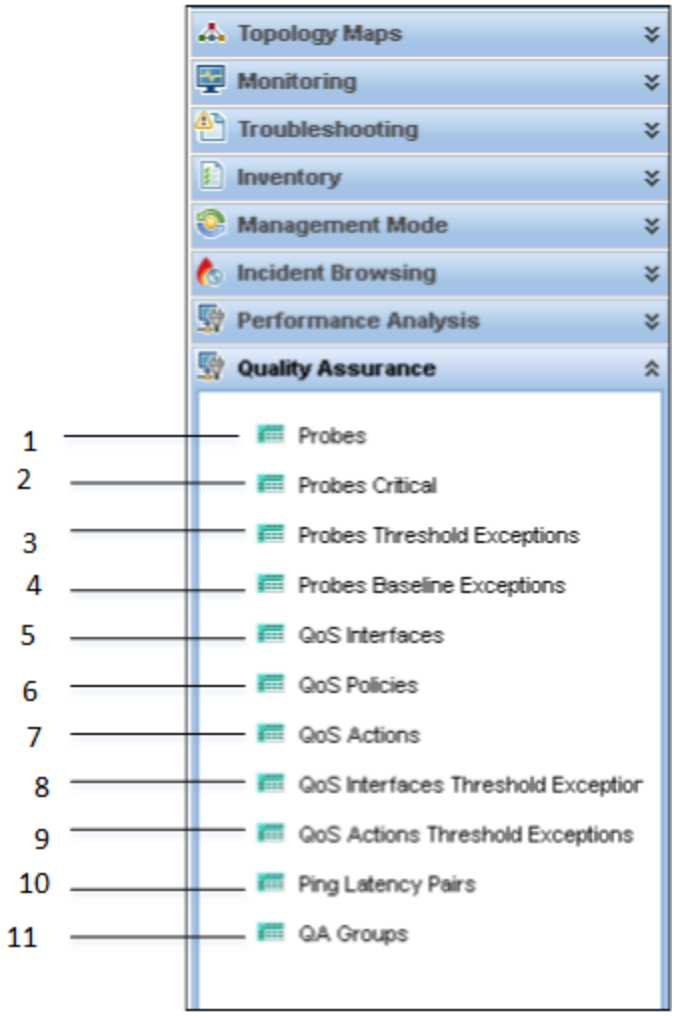
   User roles determine access to the NNMi console workspaces, forms, and actions. NNMi provides the following roles. It is not possible to create additional roles or change the names of the roles provided by NNMi:

   - 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

Filtering and Sorting Data in Inventory Views

You can filter and sort data in the workspace to categorize and view the relevant information.

The filters configured on the views are restored when the views are reopened. This is very useful as you do not have to configure the filtering option again.

To filter a column in the Quality Assurance workspace, right-click the column name and select a filtering option.

Note: Right-click the column and select **Remove Filter** to clear the filter configured on the column.

The following table displays the values based on which you can filter the QA Probes view columns:

Column Name	Allowed Filters	Disallowed Filters	Possible Values
Status	• Equals • Not equals	• Is Empty • Not Empty	• Major • Minor • No Status • Unknown • Warning • Normal • Critical • Disabled
Name	• Equals • Not equals • Is Empty • Not Empty	• less than or equal • greater than or equal	
Owner	• Equals `<value>` • Not equals `<value>` • Is Empty • Not Empty		

Column Name	Allowed Filters	Disallowed Filters	Possible Values
Service	• Equals <value> • Not equals <value>	• Is Empty • Not Empty	
Source Site	• Equals <value> • Not equals <value> • Is Empty • Not Empty	No disallowed filter	
Destination Site	• Equals <value> • Not equals <value> • Is Empty • Not Empty	No disallowed filter	
Tenant	• Equals <value> • Not equals <value> • Is Empty • Not Empty	No disallowed filter	
RTT	• Equals <value> • Not equals <value> • Is Empty* • Not Empty* * Available only when a RTT value is chosen.	• Contains • Matches	

Column Name	Allowed Filters	Disallowed Filters	Possible Values
Jitter	• Equals <value> • Not equals <value> • Is Empty** • Not Empty** ** Available only when a Jitter value is chosen.	• Contains • Matches	
Packet Loss	• Equals <value> • Not equals <value> • Is Empty*** • Not Empty*** *** Available only when a Packet Loss value is chosen.	• Contains • Matches	
Manager	• Equals <value> • Not equals <value> • Is Empty • Not Empty	No disallowed filter	

NNM iSPI Performance for QA enables you to create customized filters using the Create Filter utility. You can use this utility on all the columns.

To create a custom filter, follow these steps:

1. Select a column heading, right-click, and then select **Filter > Create Filter...**
2. Select one or more values for Equals or Not Equals filters.

   ### Equals

   When you select the option **Equals**, NNM iSPI Performance for QA filters the workspace based on the specified values.

   ### Not Equals

   When you select the option **Not Equals**, NNM iSPI Performance for QA filters the workspace based on all of the specified values.
3. Click **Apply**.

Example 1

If you want to display the QA probes with a high Round Trip Time (RTT) or high Packet Loss, then you can create a filter for the RTT column that specifies "`Equals High`" and a filter for the Packet Loss column that specifies "`Equals High`". The workspace filters and displays only those QA probes with:

- High RTT
- High packet loss
- Both high RTT and packet loss

Example 2

If you want to display the QA probes that neither have a high Round Trip Time (RTT) nor high Packet Loss, then you can create a filter for the RTT column that specifies "`Not Equals High`" and a filter for the Packet Loss column that specifies "`Not Equals High`". The workspace filters and displays only those QA probes that neither have high RTT nor high packet loss.

Sorting Data in the Inventory Views

You can sort a workspace column in ascending or descending order.

Sorting is enabled only for limited columns.

By default, the workspace is sorted based on the Status column.

To sort a column in the Quality Assurance workspace, right-click the column name and select a sorting option.

Multi-Tenancy Architecture in the NNM iSPI Performance for QA

The NNM iSPI Performance for QA supports multi-tenant architecture configured in NNMi. In NNMi, a tenant is the top-level organization to which a node belongs. Tenants enable you to partition your network across multiple customers. The NNMi administrator can restrict visibility and control to parts of the network for some or all operators. This feature restricts the access to certain objects such as QA Probes, Sites, and QoS elements in NNM iSPI Performance for QA based on the tenant configuration, security group configuration, and user group configuration in NNMi.

The security group defined for a node in NNMi is also applicable for the QA probes and QoS elements hosted on the node. This implies that all QA probes and QoS elements cannot be viewed by all users either in a table view or a form view. For example, if a user has access to a set of nodes, the user can view only the QA probes and QoS elements configured on those nodes.

A user can view a source site and destination site only if at least one of the QA probes or QoS elements associated with the source site can be accessed by the user. A user can view the site map only if any one of the QA probes or QoS elements of the site can be accessed by the user. In addition, a user can view the Real Time Line graph only if the source node or the QA probe can be accessed by the user.

A user cannot view all the incidents. A user can view only those incidents whose source node, QA probe, or QoS element can be accessed by the user.

Multi-tenancy is also applicable for the Network Performance Server and restricts a user to view reports on only selective QA probes and QoS elements. For example, while generating Top N report, a user can view the report for the probes and QoS elements that can be accessed by the user.

Multi-tenant architecture establishes a node to tenant association and determines the nodes that can be accessed by the user. As an administrator, you can configure the QA probes for a source node irrespective of whether you can access the destination node.

An administrator can create, update, and delete all configurations.

See the topic *Configuring Security* in the *NNMi Online Help* for more information on Tenants and Security Groups.

Quality Assurance Performance Dashboard

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.

QA Performance Dashboard View, continued

Dashboard Item	Display Type	Description
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 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.

QA Performance Dashboard View, continued

Dashboard Item	Display Type	Description
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.

NNM iSPI Performance for 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 (Supported by HP H3C devices)
- Oracle
- TCP Connect (Supported by HP H3C devices)
- UDP Echo (Supported by HP H3C devices)
- PATH 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 traffic 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.

Accessing the QA Probes Inventory View

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 **Quality Assurance** in the Workspaces panel. The Quality Assurance tab expands, displaying the QA Probes view.
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	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 one of the following statuses : • Normal • Warning • Major

[1]Some examples of network elements are routers and switches.

Attribute Name	Description
	• Critical • Unknown • Disabled • Not Polled • No Status For more information on status, see the topic QA Probe Status.
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. Some of the QA probe types that the NNM iSPI Performance for QA recognizes are: • UDP Echo • ICMP Echo • UDP • TCP Connect • VoIP • HTTP • DNS • DHCP • Oracle • HTTPS
Source	The source device in which the probe is configured.
Destination	The destination network device till which the probe is configured.

Attribute Name	Description
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	The round-trip time used by the selected QA probe. Displays one of the following threshold states for the metric: High Nominal Low Not Polled Unavailable Threshold Not Set None
Jitter	The delay[2] 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:

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

Attribute Name	Description
	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:

Threshold States

State	Description
High	*For Count-Based Threshold Configuration:* 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. *For Time-Based Threshold Configuration:* 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.
Low	*For Count-Based Threshold Configuration*: 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. *For Time-Based Threshold Configuration:* 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. Typically, this threshold state is applicable for metrics such as Mean Opinion Score (MOS).

Threshold States, continued

State	Description
Not Polled	Indicates that the metric is intentionally not polled. Some of the possible reasons are: • The parent Node or Interface is set to Not Managed or Out of Service. • The metric is not supported for the particular entity. 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".
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	*For Count-Based Threshold Configuration:* Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count. *For Time-Based Threshold Configuration:* 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).

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 µs), two-way jitter (ms or µs), 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	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

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	Status of the QA probe. A QA probe can have one of the following statuses: • No Status • Normal • Disabled • Unknown • Warning • Major • Critical For more information about QA probe status, see QA Probe Status.
Name	Name of the selected QA probe. For QA probes, the QA probe name is derived from the 'TAG' field of the QA probe definition. If the tag field is not present, then the QA probe name is derived by appending the source node name, the target IP address, and the admin index. For RFC QA probes, the name is derived from the RFC MIB. The QA probe names cannot be blank.
Owner	Name of the QA probe owner.
Service	Type of the QA probe.

Basic Attributes: QA Probe Details, continued

Attribute	Description
	Possible service types are: • UDP Echo • ICMP Echo • UDP • TCP Connect • VoIP • HTTP • DNS • HTTPS • Oracle • DHCP
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.

Source/Destination Info

This section displays the following:

Basic Attributes: Source/Destination Info

Attribute	Description
Source	Name of the starting device from which the QA probe is configured. Click  to display the source node information. The Node: <Node Name> form opens. Select the **QA Probes** tab to display the QA probes initiated from this node.
Source IP Address	IP address of the starting device from which the QA probe is configured.

Basic Attributes: Source/Destination Info, continued

Attribute	Description
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.
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 for the last discovery.

Basic Attributes: Source/Destination Info, continued

Attribute	Description
Management Mode	Whether the source node is managed or not. Possible states are as follows: • 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".

QA Probes Form: State Tab

The **State** tab 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.

QA Probes Form: Threshold State Tab

The **Threshold State** tab 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.

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	The threshold state of the probe. The valid threshold states are listed below: High Nominal Low Not Polled Unavailable

[1]Some examples of network elements are routers and switches.

Field Name	Description
	Threshold Not Set None For more information about the threshold states, see the topic Threshold States.
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	*For Count-Based Threshold Configuration:* 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. *For Time-Based Threshold Configuration:* 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

Threshold States, continued

State	Description
	Duration Window.
Nominal	Indicates that the measured value of the metric is within the normal healthy range.
Low	*For Count-Based Threshold Configuration*: 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. *For Time-Based Threshold Configuration:* 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. Typically, this threshold state is applicable for metrics such as Mean Opinion Score (MOS).
Not Polled	Indicates that the metric is intentionally not polled. Some of the possible reasons are: • The parent Node or Interface is set to Not Managed or Out of Service. • The metric is not supported for the particular entity. 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".
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	*For Count-Based Threshold Configuration:* Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count. *For Time-Based Threshold Configuration:* 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).

- 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.

QA Probes Form: Baseline State Tab

The **Baseline State** tab 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.

QA Probes Form: Status Tab

The **Status** tab 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	Overall status for the current QA probe Possible values are: • No Status • Normal • Disabled • Unknown • Warning • Major

Attribute: Status Tab, continued

Attribute	Description
	• Critical For more information on the QA probe status, see the topic QA Probe Status. 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. See the following topics for information about how the current status was determined: • QA Probes Form: State Tab • QA Probes Form: Conclusions Tab
Status Last Modified	Current status is calculated and set by Causal Engine. The Time Stamp data displays the time when the status of the QA probe is last updated.
Status History	List of up to the last 30 changes in status for the selected QA probe. 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. • Click  **Refresh** to refresh the Status History table. • Click  **Show View in New Window** to open the Status History table in an independent window.

QA Probes Form: Conclusions Tab

The **Conclusions** tab 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	Status of the conclusion. Possible values are: • No Status • Normal • Disabled • Unknown • Warning • Major • Critical For more information on the QA probe status, see the topic QA Probe Status. Status reflects the most serious outstanding conclusion.
Time Stamp	Displays the time when the status of the QA probe was last updated.
Conclusions	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. 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. Examples of conclusions that might appear together are listed below: • TestUp[1] • RttThresholdStateHigh • TwoWayPktLossThresholdStateHigh Following examples list some of the conclusions caused by Administrative and Operational states:

[1]When both Administrative and Operational states are up.

Attribute: Conclusions Tab, continued

Attribute	Description
	Conclusions caused by Administrative State TestTransient • notready • createandwait • createandgo • destroy TestDisabled • disabled • Notinservice TestUnknown Caused by an SNMP error. TestUnpolled Caused when the QA probe is not polled. **Conclusions caused by Operational State** TestFailed • OperStateTimeout on probe • OperStateDisconnected on probe • OperStateNotConnected on probe • OperStateApplicationSpecific on probe • OperStateDnsServerTimeout on probe • OperStateTcpConnectTimeout on probe • OperStateHttpTransactionTimeout on probe

Attribute: Conclusions Tab, continued

Attribute	Description
	• OperStateDnsQueryError on probe • OperStateHttpError on probe • OperStateError on probe • OperStateDisabled on probe TestError OperStateOther on probe OperStateSequenceError on probe OperStateOverThreashold on probe OperStateBusy on probe OperStateVerifyError on probe OperStateDropped on probe For information about how conclusions are based on the QA Probe States, see QA Probes Form: State Tab.

QA Probes Form: Incidents Tab

The **Incidents** tab 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	The attributes listed in the incidents tab are same as the ones available in the NNMi Incidents form. For more information about the Incidents attributes, see the topic *NNMi Incidents Form* in the *Network Node Manager i Software Online help.* NNM iSPI Performance for QA generates the following incidents: TwoWayJitterHigh Indicates a high two-way jitter value (which is the average of the following values): • 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
	SourceToDestinationPositiveJitterHigh 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.
	DestinationToSourcePositiveJitterHigh 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.
	SourceToDestinationNegativeJitterHigh 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.
	DestinationToSourceNegativeJitterHigh 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 the whether the latest value is polled or cumulative value is polled.
	TwoWayPacketLossHigh Indicates a high percentage of two-way packet loss. This value is the average of the following values: • Packet loss percentage from the source to the destination • Packet loss percentage from the destination to the source

Attribute: Incidents Tab, continued

Attribute	Description
	SourceToDestinationPacketLossHigh Indicates a high percentage of packet loss from the source to the destination. The packet loss percentage is calculated from the ratio of the total number of packets sent to the reported number of packets lost. The exact MIB values that are queried vary based on whether the latest value is polled or cumulative value is polled.
	DestinationToSourcePacketLossHigh Indicates a high percentage of packet loss from the destination to the source. The packet loss percentage is calculated from the ratio of the total number of packets sent to the reported number of packets lost. The exact MIB values that are queried vary based on whether the latest value is polled or cumulative value is polled.
	RoundTripTimeHigh 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.
	MeanOpinionScoreLow 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.
	RoundTripTimeAbnormal 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.
	TwoWayPacketLossAbnormal 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: • Packet loss percentage from the source to the destination • Packet loss percentage from the destination to the source

Attribute: Incidents Tab, continued

Attribute	Description
	TwoWayJitterAbnormal 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: • 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
	MeanOpinionScoreAbnormal 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.
	TestError This incident indicates that the QA Probe has returned an error.
	TestTransient This incident indicates that the QA Probe is in a transient state.
	TestFailed This incident indicates that the QA Probe has failed to run.
	TestDisabled This incident indicates that the QA Probe is explicitly disabled by the device administrator.

Attributes: Incidents Tab

Attribute	Description
Severity	Severity of the incident calculated by NNMi. Possible values are: • Normal • Warning • Minor • Major

Attributes: Incidents Tab, continued

Attribute	Description
	• Critical • Unknown • Disabled • Not Polled • No Status
Lifecycle State	Identifies where the incident is in the incident lifecycle.
Last Occurrence	Used when suppressing duplicate incidents or specifying an incident rate. Indicates the time when the duplicate or rate criteria were last met for a set of duplicate incidents or for a set of incidents that has a rate criteria that was met. If there are no duplicate incidents or incidents that have a rate criteria that were met, then this date is 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. 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*.

QA Probes Form: Registration Tab

The **Registration** tab 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.

QA Probes Form: HTTP(S) Tab

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.

Accessing the Critical QA Probes Inventory View

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
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.

[1] 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.

Accessing the Probes Threshold Exceptions Inventory View

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 for 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 the intricate details of threshold state violations. This view is very useful to segregate the QA probes that have violated the threshold state and to arrive 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 only the threshold violated QA probes configured on those nodes.

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	The status of the QA probes. It can be one of the following: • Warning • Major • Critical NNM iSPI Performance for QA calculates the status based on the polling status of the nodes and the threshold states. For more information on status, see the topic QA Probe Status.
Name	The name of the discovered QA probe configured in the network device.
Service	The type of the discovered QA probe.
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 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

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

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

Attribute Name	Description
	Low Not Polled Unavailable Threshold Not Set None
-ve Jitter DS	Indicates the threshold state of the negative jitter from the destination to the source. 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
Packet Loss SD	Indicates the threshold state of the percentage of packet loss from the source to the destination. Displays one of the following threshold states for the metric: High Nominal

Attribute Name	Description
	Low Not Polled Unavailable Threshold Not Set None
Packet Loss DS	Indicates the threshold state of the percentage of packet loss from the destination to source. Displays one of the following threshold states for the metric: High Nominal 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	*For Count-Based Threshold Configuration:* 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. *For Time-Based Threshold Configuration:* 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.
Low	*For Count-Based Threshold Configuration*: Indicates that the measured value of the metric is below the configured Low Value

Threshold States, continued

State	Description
	for the consecutive number of times specified in the Trigger Count. *For Time-Based Threshold Configuration:* 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. Typically, this threshold state is applicable for metrics such as Mean Opinion Score (MOS).
Not Polled	Indicates that the metric is intentionally not polled. Some of the possible reasons are: • The parent Node or Interface is set to Not Managed or Out of Service. • The metric is not supported for the particular entity. 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".
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	*For Count-Based Threshold Configuration:* Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count. *For Time-Based Threshold Configuration:* 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).

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 below.

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 µs), two-way jitter (ms or µs), 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`.

Accessing the Probes Baseline Exceptions Inventory View

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 on how baseline state is set, see the topic Baseline Monitoring.

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: • Normal • Warning

Attribute Name	Description
	• Major • Critical • Unknown • Disabled • Not Polled • No Status NNM iSPI Performance for QA calculates the status based on the polling status of the nodes and the threshold states. For more information on status, see the topic QA Probe Status.
Name	The name of the discovered QA probe configured in the network device.
Service	The type of the discovered QA probe.
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 one of the following baseline states for the metric: • 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.

Attribute Name	Description
Two Way Jitter	Indicates two way jitter. This value is the average of the following values: • 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 Displays one of the following baseline states for the metric: • 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.
Two Way Packet Loss	The percentage of packets that failed to arrive from the source to destination and destination to source. Displays one of the following baseline states for the metric: • 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
MOS	Indicates the baseline state of Mean Opinion Score (MOS) of the jitter. Displays one of the following baseline states for the metric: • 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.

Viewing and Saving the QA Probes associated with QA Groups Using Command Line Utilities

To display and save 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	`$NnmInstallDir/bin/nmsqacustomgrouputil.ovpl -u <username> -p <password> -display -gt QAProbes -g <QA group name>`	
Windows	`%NnmInstallDir%\bin\nmsqacustomgrouputil.ovpl -u <username> -p <password> -display -gt QAProbes -g <QA group name>`	
QoS		
Linux	`$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>`	
Windows	`%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>`	

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	`$NnmInstallDir/bin/nmsqacustomgrouputil.ovpl -u <username> -p <password> -gt qaprobes -g <QA group name> -savetofile <filename>`	
Windows	`%NnmInstallDir%\bin\nmsqacustomgrouputil.ovpl -u <username> -p <password> -gt qaprobes -g <QA group name> -savetofile <filename>`	
QoS		
Linux	`$NnmInstallDir/bin/nmsqacustomgrouputil.ovpl -u <username> -p <password> -gt CBQOS -g <custom group name> -<interface/action> -savetofile <filename>`	
Windows	`%NnmInstallDir%\bin\nmsqacustomgrouputil.ovpl -u <username> -p <password> -gt CBQOS -g <custom group name> -<interface/action> -savetofile <filename>`	

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

Viewing Source Interface for a QA Probe

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 Softwarehas 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 Configure Probes.

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.

QA Probe Status

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: • Other • Over the threshold value • Busy • Not Connected • Dropped	The probe has returned one of the following statuses: • 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: • 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.

Status	Description for Operators	Description for Administrators
Unknown	The probe has returned one of the following errors: • 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: • Not in service • 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	• 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.	• 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.

NNM iSPI Performance for QA 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.

NNM iSPI Performance for QA 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.

Administrative State

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

QA Probe State Attributes	Description
rttMonCtrlAdminStatus	The status of the conceptual RTT control row. The current Administrative State contributes towards the status calculation for this QA probe. Possible values are: • active[1] • notInService[2] • notReady[3] • createAndGo[4] • createAndWait[5] • destroy[6]

RFC QA Probe or Juniper RPM QA Probe State Attributes	Description
pingCtlAdminStatus	For RFC, the following values are supported for the Administrative State: • Enabled[7] • Disabled[8]

[1]Indicates that the conceptual row is available for use by the managed device.
[2]Indicates that the conceptual row exists in the agent, but is unavailable for use by the managed device.
[3]Indicates that the conceptual row exists in the agent, but is missing information necessary in order to be available for use by the managed device.
[4]Supplied 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.
[5]Supplied 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.
[6]Supplied by a management station that wants to delete all of the instances associated with an existing conceptual row.
[7]Attempt to activate the QA probe.
[8]Deactivate the QA probe.

Operational State

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

QA Probe State Attributes	Description
• rttMonLatestJitterOperSense • rttMonLatestRttOperSense	The rttMonLatestJitterOperSense status defines an application specific sense code for the completion status of the latest Jitter RTT operation. The rttMonLatestRttOperSense status defines an application sense code for the completion status of the latest RTT operation. The current Operational State contributes towards the status calculation for this QA probe. The possible values and their descriptions are given in the below table.

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.

Possible Values	Description
applicationSpecific(10)	The application generating the operation had a specific error.
dnsServerTimeout(11)	DNS Server Timeout
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: • Enabled[1] • Disabled[2]

[1]QA probe is active.
[2]QA probe has stopped.

NNM iSPI Performance for QA Quality of Service (QoS)

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.

Accessing the QoS Interfaces Inventory View

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.

Attribute Name	Description
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: • 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: • 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.

[1]In Policy defines the policy which is applied to the incoming traffic.
[2]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.
[3]Out Policy defines the policy which is applied to the outgoing traffic.
[4]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.

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 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 theNNM 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.

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 of the selected QoS Interface, in the form of graphs. The graph shows the following:

- Interface utilization of the selected QoS Interface.
- Bandwidth utilization of the selected QoS Interface.
- Availability of the selected QoS Interface. It denotes whether the interface is active or not.
- Pre-policy rate and Post-policy rate of the selected QoS Interface.

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 QoS interface enables you to easily determine the root cause of the fault.

The following table indicates the status information:

QoS Interface Status	Status color indicated 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

QoS Interface Form: In Policy Tab

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: • 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 details about CBQoS class map for a selected traffic class, see QoS Class Map Form.

[1]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.
[2]The policy that the parent policy refers to.

QoS Interfaces Form: Out Policy Details Tab

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

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: • 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.

[1]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.
[2]The policy that the parent policy refers to.

QoS Interfaces Form: Classifiers Tab

The **Classifier** tab displays information about the classifier applied on the selected interface.

Attributes: Classifiers Tab

Attribute	Description
Name	The name of the classifier applied on the interface.

This tab appears only when the classifier is applied on the selected interface of the Juniper device.

QoS Interfaces Form: Queue Association Tab

The **Queue Association** tab displays information about the traffic (forwarding) class name and the associated queue number on the selected interface. A queue number can be associated to one or more traffic classes.

Attributes: Queue Association Tab

Attribute	Description
Traffic Class Name	The name of the traffic class.
Queue Number	The queue number to which the traffic class on the selected interface is associated.

This tab appears only when an interface on the Juniper node is selected.

QoS Interfaces Form: Threshold State Tab

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

It displays the threshold states for the parent policy[1] as well as the child policy[2].

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.

Attributes: Threshold State Tab

Attribute	Description
State	Threshold state for the QoS elements. Can be one of the following values: • High:[3] • Nominal:[4] • Not Defined:[5]
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.

[1]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.
[2]The policy that the parent policy refers to.
[3] Specifies that the metric value for the QoS policy crossed the configured threshold value.
[4] Specifies that the metric value for the QoS policy is within the configured threshold value.
[5]Specifies that the threshold was configured, but NNM iSPI Performance for QA did not poll the device.

Attributes: Threshold State Tab, continued

Attribute	Description
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: 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: • Count: [1] • Time: [2]
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.

[1]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.
[2]NNM iSPI Performance for QA raises an incident only if the metric value is beyond the threshold value for a pre-specified time period.

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: • 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 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.

Attributes: Incidents Tab, continued

Attribute	Description
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 Interfaces Inventory: 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.

QoS In or Out Policy Form

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.

Accessing the QoS Policies Inventory View

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.

[1]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.
[2]The policy that the parent policy refers to.

Attribute Name	Description
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: • 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 QoS Policies Form: Traffic Classes Tab.

QoS Policies Form: Interface Tab

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.
Applied On	The interface on which the policy is applied. Possible values are: • Control Plane • Interface • Sub Interface
Management Server	Specifies whether the NNMi management server is local or specifies the name of the regional manager.

[1] In Policy defines the policy which is applied to the incoming traffic.
[2] Out Policy defines the policy which is applied to the outgoing traffic.

QoS Policies Form: Traffic Classes Tab

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	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.

[1]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.
[2]The policy that the parent policy refers to.

Attributes: Traffic Classes Tab, continued

Attribute	Description
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 Policies Form: QoS Policy Hierarchy Tab

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 QoS Policies Form: Traffic Classes Tab.

Accessing the QoS Actions Inventory View

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	The threshold state for the action. Can be one of the following values: **Threshold States** **State** / **Description** High — *For Count-Based Threshold Configuration:* 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. *For Time-Based Threshold Configuration:* Indicates that the measured value of the metric is above the configured High Value and this

[1]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.
[2]The policy that the parent policy refers to.

<table>
<tr><th>Attribute Name</th><th>Description</th></tr>
<tr><td></td><td>Threshold States, continued
<table>
<tr><th>State</th><th>Description</th></tr>
<tr><td></td><td>high value persists for the specified High Duration within the High Duration Window.</td></tr>
<tr><td>Nominal</td><td>Indicates that the measured value of the metric is within the normal healthy range.</td></tr>
<tr><td>Unavailable</td><td>Unable to compute the metric or the computed value is outside the valid range.</td></tr>
<tr><td>Threshold Not Set</td><td>Indicates that the threshold is not set for the metric.</td></tr>
<tr><td>None</td><td>For Count-Based Threshold Configuration:

Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count.

For Time-Based Threshold Configuration:

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).</td></tr>
</table></td></tr>
<tr><td>Action</td><td>The type of Action applied. Possible values are:
Policing
Shaping
Queuing
Packet Marking
RED</td></tr>
<tr><td>Traffic Class Name</td><td>Name of the Traffic Class associated with the selected action.</td></tr>
<tr><td>Policy Name</td><td>The name of the policy applied.</td></tr>
<tr><td>Direction</td><td>Indicates whether the policy was applied on the incoming or outgoing traffic for an interface.</td></tr>
<tr><td>Queue Number</td><td>Indicates the queue number to which the traffic (forwarding) class (on which the action is configured) is associated.

This field is applicable only for Juniper devices.</td></tr>
</table>

Attribute Name	Description
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.
Management Mode	Specifies whether the source node is managed or not. Possible states are as follows: • 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 Tab (Analysis Panel).

Threshold States Tab (Analysis Panel)

The **Threshold State** tab in the Analysis panel 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 NNM iSPI Performance for QA QoS Threshold Configuration.

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: • High[1] • Nominal[2]
Type	Type of the threshold set for the metric. Can be of the following types: • Count[3] • Time[4]
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

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

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.

QoS Actions Form: Interface Tab

The **Interface** tab 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.
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: • 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: • 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.

[1] In Policy defines the policy which is applied to the incoming traffic.
[2] Out Policy defines the policy which is applied to the outgoing traffic.

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.

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 Actions Form: QoS Policies Tab

The **QoS Policies** tab 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 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: • 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.

Accessing the QoS Interfaces Threshold Exceptions Inventory View

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 QoS Actions.

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.** Tthe 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.

[1]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.

Attribute Name	Description
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.
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	*For Count-Based Threshold Configuration:* 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. *For Time-Based Threshold Configuration:* 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.

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	*For Count-Based Threshold Configuration:* Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count. *For Time-Based Threshold Configuration:* 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).

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 Accessing the QoS Interfaces Inventory View.

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 QoS Actions.

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	The threshold state for the action. Can be any of the following values: **Threshold States** **State** / **Description** High: *For Count-Based Threshold Configuration:* 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. *For Time-Based Threshold Configuration:* 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.

<table>
<tr><th>Attribute Name</th><th>Description</th></tr>
<tr><td></td><td>Threshold States, continued
<table>
<tr><th>State</th><th>Description</th></tr>
<tr><td>Unavailable</td><td>Unable to compute the metric or the computed value is outside the valid range.</td></tr>
<tr><td>Threshold Not Set</td><td>Indicates that the threshold is not set for the metric.</td></tr>
<tr><td>None</td><td>For Count-Based Threshold Configuration:

Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count.

For Time-Based Threshold Configuration:

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).</td></tr>
</table></td></tr>
<tr><td>Action</td><td>The name of the action that crossed the threshold.</td></tr>
<tr><td>Traffic Class Name</td><td>Name of an Traffic Class associated with the selected action.</td></tr>
<tr><td>Policy Name</td><td>The name of the policy associated with the selected action.

By default, this attribute displays only the parent policy[1] name.</td></tr>
<tr><td>Direction</td><td>Indicates whether the policy is applied on the incoming traffic or outgoing traffic for the selected interface.</td></tr>
<tr><td>Interface Name</td><td>The name of the interface associated with the selected action</td></tr>
<tr><td>Hosted on Node</td><td>The name of the node on which the interface resides</td></tr>
<tr><td>Tenant</td><td>Specifies the NNMi tenant selected for the node (specified in Hosted On Node attribute)</td></tr>
<tr><td>Management Server</td><td>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.</td></tr>
</table>

[1]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.

Attribute Name	Description
Management Mode	Specifies whether the source node is managed or not Possible states are as follows: • 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	*For Count-Based Threshold Configuration:* 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. *For Time-Based Threshold Configuration:* 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	*For Count-Based Threshold Configuration:* Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count. *For Time-Based Threshold Configuration:* 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).

To open the QoS Action inventory view for an interface, select the interface and click **Open**. For information about QoS Action inventory view, see Accessing the QoS Actions Inventory View.

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.

NNM iSPI Performance for QA 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.

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	(Queue Depth/Maximum Queue Depth) * 100	QueueUtilizationHigh	Major
Queue Bandwidth Utilization	(PostPolicyBytesPerSecond (per class)/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

Accessing the QA Groups Inventory View

Tip: See "QA Groups" on page 297 for more details about QA groups.

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. • 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.

QA Groups Form

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:

- "QA Groups Form: Probes Tab" on the next page
- "QA Groups Form: Probes Critical Tab" on page 124
- " QA Groups Form View: Probes Threshold Exception Tab" on page 125
- "QA Groups Form: Probes Baseline Exceptions Tab" on page 130
- "QA Groups Form: Registration Tab" on page 134

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

- "QA Groups Form: QoS Interfaces Tab" on page 135
- "QA Groups Form: QoS Actions Tab" on page 136
- "QA Groups Form: QoS Interfaces Threshold Exceptions Tab" on page 137
- "QA Groups Form: QoS Actions Threshold Exceptions Tab" on page 139
- "QA Groups Form: Registration Tab" on page 142

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

- "QA Groups Form: Ping Latency Pairs Tab" on page 143"
- "QA Groups Form: Registration Tab" on page 145

QA Groups Form: Probes Tab

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	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: • Normal • Warning • Major • Critical • Unknown • Disabled • Not Polled • No Status For more information about status, see the topic QA Probe Status.
Name	The name of the discovered QA probe configured in the network device.
Owner	The name of the discovered QA probe's owner.

Attribute Name	Description
Service	The type of the discovered QA probe. Some of the QA probe types that the NNM iSPI Performance for QA recognizes are as follows: • 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: High Nominal Low Not Polled Unavailable Threshold Not Set None

Attribute Name	Description
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 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.

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

QA Groups Form: Probes Critical Tab

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	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 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. Some of the QA probe types that the NNM iSPI Performance for QA recognizes are as follows: • 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 NNMi tenant selected for the network device.

QA Groups Form View: Probes Threshold Exception Tab

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: • 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 NNM iSPI Performance for QA recognizes are as follows: • UDP Echo • ICMP Echo • UDP • TCP Connect • VoIP • HTTP • 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.

Attribute Name	Description
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

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

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

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

Attribute Name	Description
Packet Loss SD	Indicates the threshold state of the percentage of packet loss from the source to the destination. Displays one of the following threshold states for the metric: High Nominal Low Not Polled Unavailable Threshold Not Set None
Packet Loss DS	Indicates the threshold state of the percentage of packet loss from the destination to source. Displays one of the following threshold states for the metric: High Nominal Low 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.

QA Groups Form: Probes Baseline Exceptions Tab

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: • Normal • Warning • Major • Critical • Unknown • Disabled • Not Polled • No Status For more information about status, see the topic QA Probe Status.
Name	The name of the discovered QA probe configured in the network device.

Attribute Name	Description
Service	The type of the discovered QA probe. Some of the QA probe types that the NNM iSPI Performance for QA recognizes are as follows: • UDP Echo • ICMP Echo • UDP • TCP Connect • VoIP • HTTP • 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 baseline states for the metric: •  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.

Attribute Name	Description
Two Way Jitter	Indicates two way jitter. This value is the average of the following values: • 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 Displays one of the following baseline states for the metric: •  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.
Two Way Packet Loss	The percentage of packets that failed to arrive from the source to destination and destination to source. Displays one of the following baseline states for the metric: •  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
MOS	Indicates the baseline state of the Mean Opinion Score (MOS) of the jitter. Displays one of the following baseline states for the metric: •  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

QA Groups Form: Registration Tab

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*

QA Groups Form: QoS Interfaces Tab

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: • Control Plane • Interface
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: • 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.

[1] In Policy defines the policy which is applied to the incoming traffic.
[2] Out Policy defines the policy which is applied to the outgoing traffic.

QA Groups Form: QoS Actions Tab

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

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

Attribute Name	Description
Action	The type of Action applied. Possible values are: • 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: • 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.

QA Groups Form: QoS Interfaces Threshold Exceptions Tab

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.

Attribute Name	Description
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	*For Count-Based Threshold Configuration:* 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. *For Time-Based Threshold Configuration:* 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	*For Count-Based Threshold Configuration:* Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count. *For Time-Based Threshold Configuration:* 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).

QA Groups Form: QoS Actions Threshold Exceptions Tab

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 QoS Actions.

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

<table>
<tr><th>Attribute Name</th><th>Description</th></tr>
<tr><td>State</td><td>The threshold state for the action.

The actions shows one of the following threshold states:

Threshold States
<table>
<tr><th>State</th><th>Description</th></tr>
<tr><td>High</td><td>For Count-Based Threshold Configuration:

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.

For Time-Based Threshold Configuration:

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>Nominal</td><td>Indicates that the measured value of the metric is within the normal healthy range.</td></tr>
<tr><td>Unavailable</td><td>Unable to compute the metric or the computed value is outside the valid range.</td></tr>
<tr><td>Threshold Not Set</td><td>Indicates that the threshold is not set for the metric.</td></tr>
<tr><td>None</td><td>For Count-Based Threshold Configuration:

Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count.

For Time-Based Threshold Configuration:

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).</td></tr>
</table></td></tr>
<tr><td>Action</td><td>The name of the action that crossed the threshold.</td></tr>
<tr><td>Traffic Class Name</td><td>Name of the Traffic Class associated with the selected action.</td></tr>
</table>

Attribute Name	Description
Policy Name	The name of the policy associated with the selected action. This attribute displays only the parent policies name, or only 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 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.
Management Mode	Specifies whether the source node is managed or not. Possible states are as follows: • 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.

QA Groups Form: Registration Tab

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*

QA Groups Form: Ping Latency Pairs Tab

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 : • Normal • Warning • Major • Critical • Unknown • Disabled • Not Polled • No Status For more information on status, see the topic Ping Latency Pairs Status.
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.
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.

Attribute Name	Description
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.

QA Groups Form: Registration Tab

The UUID attribute is valid for all object types. NNMi displays the UUID attribute value 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*

Analysis Pane: QA Groups

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

Chapter 1: Measuring Ping Latency Between a Router and a Node

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 (see "Ping Latency Pair Configuration" on page 314). You can also modify the default size and frequency of ping requests if you have administrator or root access to the NNMi management server (see "Configure Default Ping Attributes" on page 320).

[1] 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.

Accessing the Ping Latency Pairs Inventory View

The Ping Latency Pairs inventory view enables you to view the list of configured ping latency pair[1]s 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:

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: • 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.

[1]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.

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: • 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: • RTT (in milliseconds) • 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

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

Ping Latency Pair Form

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

Ping Pair Details

Details	Description
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*>
Status	The status of the configured ping pair. The status can be one of the following: • Normal • 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.

Ping Latency Pairs Status

The system displays any one of the following valid Ping Latency Pairs status 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: • Other • Disconnected • Over the threshold value • Busy • Not Connected • Dropped	The source node or site is Active or Enabled
Major	Indicates the metric in QA probe breaches the threshold level.	Indicates the metric in QA probe breaches the threshold level.

Status	Description for Operators	Description for Administrators
Critical	The source node has returned one of the following errors: • 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: • Not ready • Create and go • Create and wait • Destroy
Unknown	The source node has returned one of the following errors: • 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: • 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.

Status	Description for Operators	Description for Administrators
No Status	• 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 has been temporarily out of service, or should never be managed.	• 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 has been temporarily out of service, or should never be managed.

NNM iSPI Performance for QA 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.

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.

Launching the 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. You can launch the QA Group QoS Map, either for a particular QA Group or for the default QA Group.

   To launch the QA Groups QoS Map for a particular QA Group:

   a. Select **Quality Assurance → QA Groups.**

   b. Select a QA Group and select **Actions → Quality Assurance → QoS Map.**

Nodes and interfaces in the QoS map can be filtered based on three parameters, namely 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 QoS Map automatically refreshes every five minutes.

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 QoS map view for the currently selected QA Group, Traffic Class Name, Action, and Hop Count.
Refresh Status	Refreshes the status of the interfaces and edges in the QoS Map.
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.

Icon	Description
 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	Select one of the following actions from the drop-down list for which you intend to view the QoS Map: • 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 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.

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.
-  Critical - At least one of the threshold states configured on the interface is critical.

QoS Interface Link Status

- Threshold not set, Not defined - Per Class Queue Bandwidth Utilization threshold is not configured on both ends of the link.
- Critical - At least one of the Per Class Queue Bandwidth Utilization threshold states configured on the link is critical.

Launching the 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 NNMi Node Inventory:

   a. Click **Inventory** → **Nodes**.

   b. Select a node and go to step 3.

   To launch from NNMi Network Overview:

   a. Click **Topology Maps** → **Network Overview**.

   b. Select a node and go to step 3.

   To launch from QoS Interfaces Inventory:

   a. Click **Quality Assurance** → **QoS Interfaces**.

   b. Select an interface and go to step 3.

   To launch from 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 first hop neighbor for each of the QoS enabled interfaces. By default, this information is refreshed automatically every five minutes.

Nodes and interfaces displayed on the QoS neighbor map can be filtered based on three parameters, namely 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 QoS Neighbor Map view for the currently selected QA Group, Traffic Class Name, Action, and Hop Count.
Refresh Status	Refreshes the status of the interfaces and edges in the QoS Neighbor Map.
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.
Action -- Action	Select one of the following actions from the drop-down list for which you intend to view the QoS Neighbor Map: • Packet Marking • Police • Queuing • RED • Shape By default, there is no action selected.

Icon	Description
 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.

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.

NNM iSPI Performance for QA Real Time Line Graph

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.

Launching the Real Time Line Graph

Perform the following steps to launch the 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	▪ Mean Opinion Score ▪ Negative Jitter DS ▪ Negative Jitter SD ▪ Positive Jitter DS ▪ Positive Jitter SD ▪ Two Way Jitter
	Packet Loss	▪ Percentage Packet Loss DS ▪ Percentage Packet Loss SD ▪ Two Way Packet Loss %
	Round Trip Time	▪ RTT in Milliseconds ▪ RTT in Microseconds
ICMP Echo	Round Trip Time	▪ RTT in Milliseconds ▪ RTT in Microseconds
UDP Echo	Round Trip Time	▪ RTT in Milliseconds ▪ RTT in Microseconds
HTTP or HTTP(S)	Round Trip Time	▪ RTT in Milliseconds ▪ RTT in Microseconds
DHCP	Round Trip Time	▪ RTT in Milliseconds ▪ RTT in Microseconds
DNS	Round Trip Time	▪ 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].

[1]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.

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.

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

NNM iSPI Performance for QA 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.

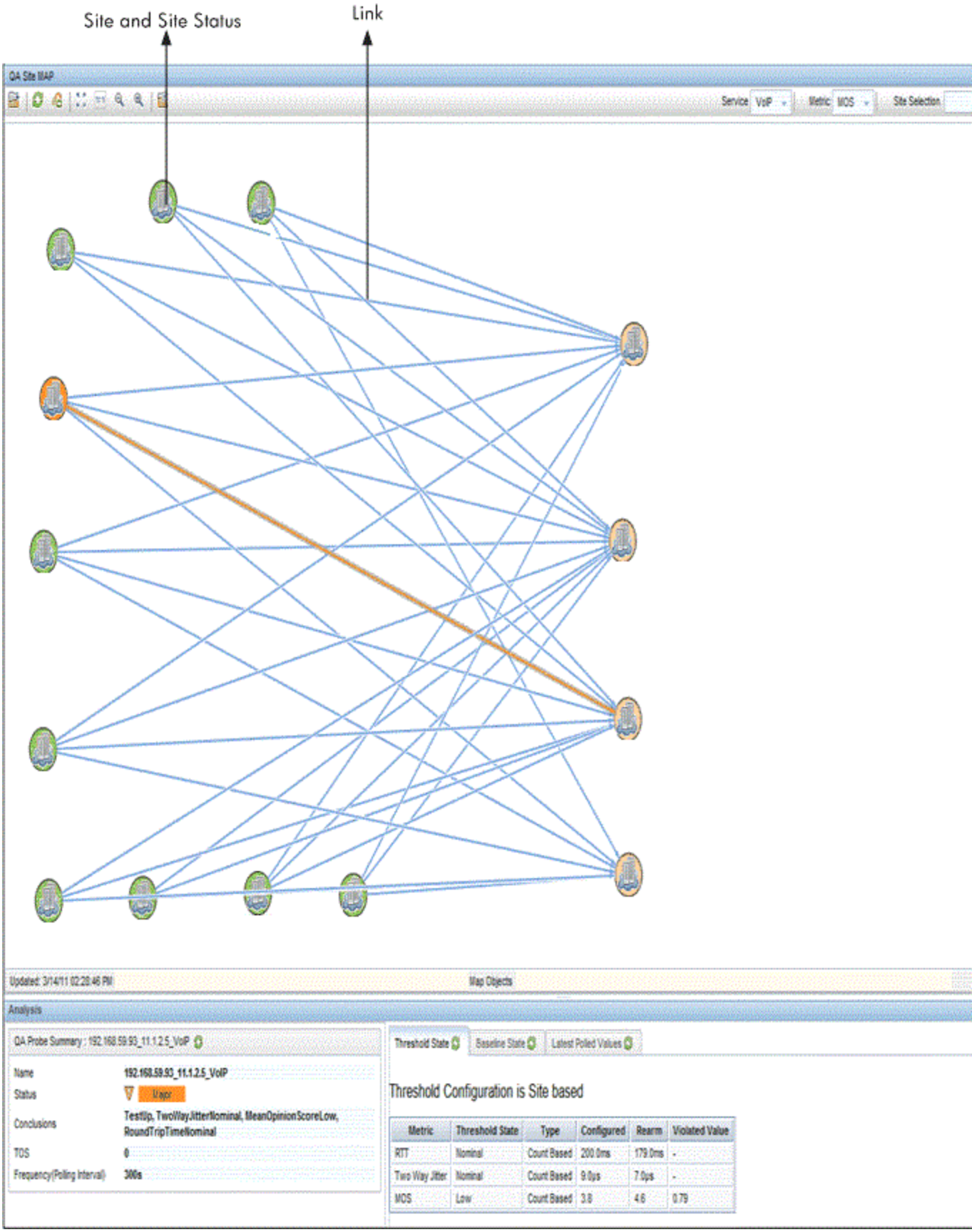
The site map represents the sites[1] as nodes, and the most severe probe status as links between the sites.

The following table lists the terminologies used in site map:

Terminology	Description
Site Status	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. 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.
Links	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. 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

Example: The following site map with the labels enable you to understand the icons used to depict the site, site status, and links in a site map.

[1] 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 and Site Status
Link
QA Site MAP
Service VoIP
Metric MOS
Site Selection
Updated: 3/14/11 02:28:46 PM
Map Objects
Analysis
QA Probe Summary : 192.168.59.93_11.1.2.5_VoIP
Name 192.168.59.93_11.1.2.5_VoIP
Status Major
Conclusions TestUp, TwoWayJitterNominal, MeanOpinionScoreLow, RoundTripTimeNominal
TOS 0
Frequency(Polling Interval) 300s
Threshold State
Baseline State
Latest Polled Values
Threshold Configuration is Site based
Metric Threshold State Type Configured Rearm Violated Value
RTT Nominal Count Based 200.0ms 179.0ms -
Two Way Jitter Nominal Count Based 9.0µs 7.0µs -
MOS Low Count Based 3.8 4.6 0.79

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
	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

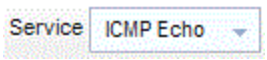
To launch the site map, follow these steps:

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 QA populates 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 QA populates 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 Available in the Site Map Toolbar	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	Select one of the following Services from the drop-down list for which you intend to view the site map:

[1]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.
[2]Links are unidirectional for the QA probes originating from the source to the destination site. The color of the link is based on the threshold state of the probe for the selected service and metric. Note: 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

Icons Available in the Site Map Toolbar	Description
	• 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	Select any one of the following metrics from the drop-down list for which you intend to view the site map: • 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 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.

Icons Available in the Site Map Toolbar	Description
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.

Click here to view a typical 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.

NNM iSPI Performance for QA Node Response View

You can view the performance of a network in a QA probe inventory view or form view. However, to understand the network performance on a more granular level, you need to assess the performance of each node that builds your network. Node Response View enables you to easily monitor the performance of any node and identify the performance of a network path.

You can view the performance of selected nodes using this map.

The Node Response View represents nodes available in the network for a selected filter criteria. The links between the nodes reflect the status of the probes running between the nodes.

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 derived based on the most severe operational status of the QA probes originating from the source node for the selected service, and metric. NNM iSPI Performance for QA displays a thick link more than one QA probe of the selected type runs between the source node and destination node. The status of the link is derived based on the most severe QA probe status.

You can view the Node Response View only if you have permissions to access at least one QA probe originating from the source node.

The node status and the Node Response View depends on your access to a set of probes originating from a selected node. If you have access to a set of probes originating from a selected node, the node status appears based on the overall status of those probes.

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 node status in a Node Response View:

Status Color	Status Description
	No Status/Disabled/Warning/Undiscovered Destination Node
	Normal

Status Color	Status Description
	Unknown NNM iSPI Performance for QA displays the node status as Unknown for the following reasons: • If the destination node is not yet polled. • If the destination node is not reachable due to router failure.
	Major
	Critical

If there are no probes configured between the source and destination node, no link appears between the source and the destination node.

The following table lists the coloring scheme of the link between two nodes (threshold state):

Link Color	Threshold / Baseline State
	High
	Nominal
	Low Applicable only if you select the following: • Service: VoIP • Metric: Mean Opinion Score (MOS)
	Threshold Not Set / Undefined / Not Polled / No Polling Policy

You can double-click on 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.

[1]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.
[2]Links are unidirectional for the QA probes originating from the source to the destination site. The color of the link is based on the threshold state of the probe for the selected service and metric. Note: 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

Icons	Description
 Refresh Status	Refreshes only the node status in the Node Response View.
Type	Select one of the following options: • Between[1] • Source Centric[2] • Destination Centric[3]
Service	Select one of the following Services from the drop-down list: • DNS • HTTP • HTTPS • ICMP Echo (Default) • ORACLE • TCP Connect • UDP Echo • UDP Jitter • VoIP
Metric	Select one of the following metrics: • + ve Jitter • -ve Jitter • Availability (Default) • MOS

[1] Enables the Node Response View to display bi-directional links between the selected source and destination nodes.
[2] Enables the Node Response View to display links from the selected source node and all the destination nodes. This is the default selection.
[3] Enables the Node Response View to display links between the selected destination node and the source node.

Icons	Description
	• RTT • Two Way Jitter • Two Way Packet Loss • +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.
 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.

NNM iSPI Performance for QA 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 selected nodes.

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

The following table lists the terminologies used in 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	The status and coloring scheme of the links is derived based on the most severe operational status of the QA probes originating from the source node for the selected service, and metric. NNM iSPI Performance for QA displays a thick link more than one QA probe of the selected type runs between the source node and destination nodes. The status of the link is derived based on the most severe QA probe status.

The node status and the Global Node Response View depends on whether you have access to a set of probes originating from a node. If you have access to a set of probes originating from a node, the node status appears based on the overall status of those probes.

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 node status in a Global Node Response View:

Status Color	Status Description
	No Status/Disabled/Warning/Undiscovered Destination Node
	Normal
	Unknown NNM iSPI Performance for QA displays the node status as Unknown for the following reasons: • If the destination node is not yet polled. • If the destination node is not reachable due to router failure.

Status Color	Status Description
	Major
	Critical

If there are no probes configured between the source and destination node, no link appears between the source and the destination node.

The following table lists the coloring scheme of the link between two nodes (threshold state):

Link Color	Threshold / Baseline State
	High
	Nominal
	Low Applicable only if you select the following: • Service: VoIP • Metric: Mean Opinion Score (MOS)
	Threshold Not Set / Undefined / Not Polled / No Polling Policy

You can double-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.

[1]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.
[2]Links are unidirectional for the QA probes originating from the source to the destination site. The color of the link is based on the threshold state of the probe for the selected service and metric. Note: 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

Icons	Description
Type	Select one of the following options: • Between[1] • Source Centric[2] • Destination Centric[3]
Service	Select one of the following Services from the drop-down list: • DNS • HTTP • HTTPS • ICMP Echo (Default) • Oracle • TCP Connect • UDP Echo • UDP Jitter • VoIP • DHCP
Metric	Select one of the following metrics: • + ve Jitter • -ve Jitter • Availability (Default) • MOS • RTT

[1] Enables the Global Node Response View to display bi-directional links between the selected source and destination nodes.
[2] Enables the Global Node Response View to display links from the selected source node and all the destination nodes. This is the default selection.
[3] Enables the Global Node Response View to display links between the selected destination node and the source node.

Icons	Description
	• Two Way Jitter • Two Way Packet Loss • +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.
 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.

Root Cause Analysis for 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.

Correlated Incidents

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

NNM iSPI Performance for QA Application Health Report

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

Launching the QA 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 2: NNM iSPI Performance for QA 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

[1] 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.

NNM iSPI Performance for QA Quality Assurance 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

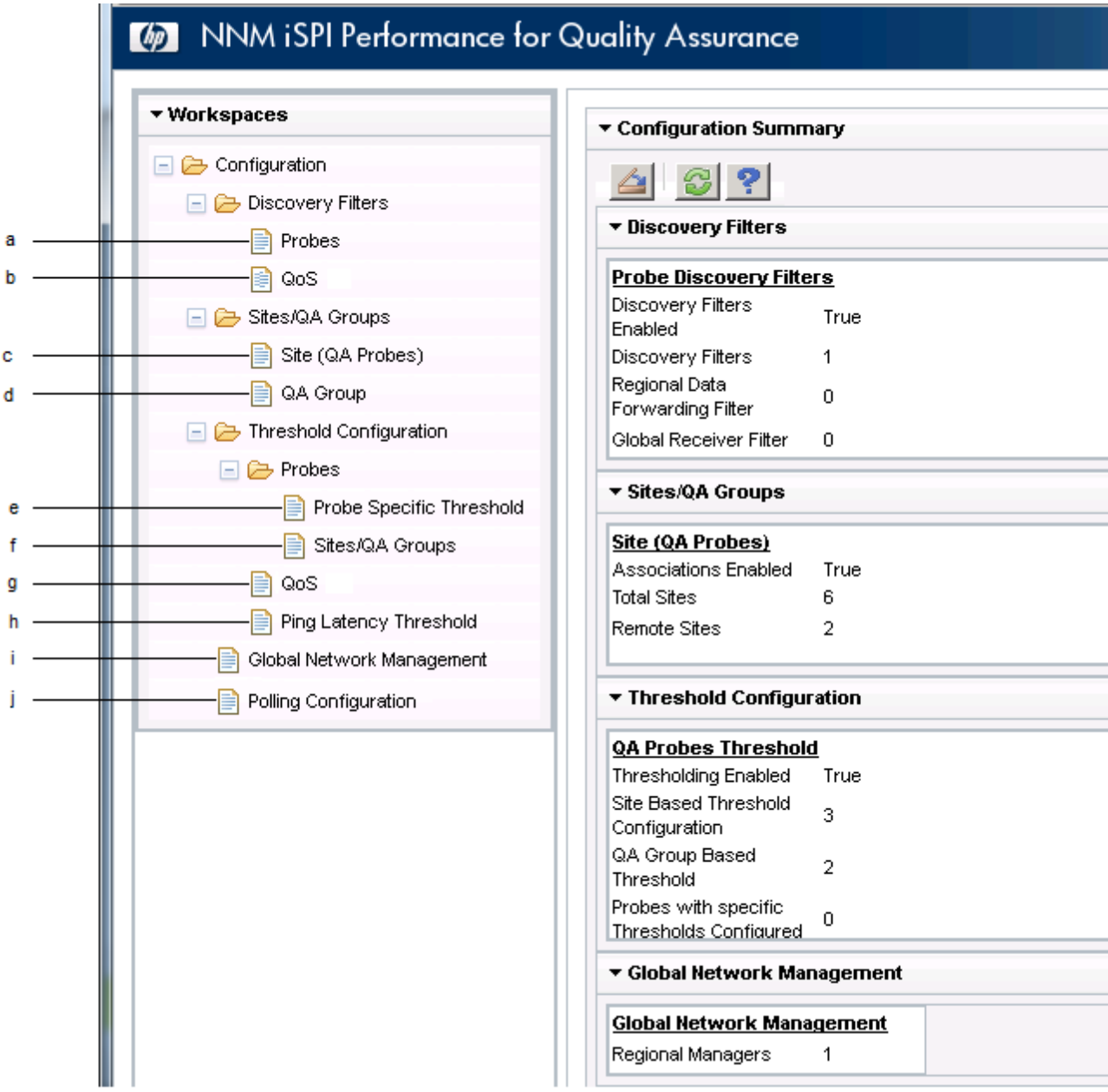
To launch the Quality Assurance Configuration console:

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**

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**

[1]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.
[2]Sites exported from the regional manager to the global manager are known as Remote Sites.
[3]Sites exported from the regional manager to the global manager are known as Remote Sites.

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:

   `%nnmdatadir%\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. `nnmsso.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 Guide*.

Configuring 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 preconfigured 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	How
Launch the probe configuration form	Launching the probe configuration form
Configure Probes	Configuring QA Probes
Deploy Probes	Deploying QA Probes
View Deployment Status	Viewing the deployment status
View Preconfigured Probes	Viewing the preconfigured probes
Create a Template	Creating a Template
View a Probe List	Viewing a Probe List
View a Template List	Viewing a Template List

Discovering QA Probes Using the nmsqadisco.ovpl Command

NNM iSPI Performance for QA discovers the QA probes configured in the network managed by NNMi during each NNMi discovery.

Use 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.

Configuring QA Probes Using nmsqaprobeconfig.ovpl Command

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)
- PATH Echo (supported by Cisco only)
- 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, path echo, 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 Using Command-Line Utility

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.tmpl` 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.

Launching the Probe Configuration Form

Perform the following steps to launch the Probe Configuration form:

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

   You must have administrator privileges.

2. You can launch the Probe Configuration form from the Nodes Inventory, Network Overview, Interfaces Inventory or IP Addresses inventory view.

   To launch the Probe Configuration form from the Nodes Inventory

   a. Click **Inventory** → **Nodes.**

   b. From the Nodes inventory, select the nodes you want to configure the QA probes on.

   c. Go to step 3.

   To launch the Probe Configuration form from the Network Overview

   a. Click **Topology Maps** → **Network Overview.**

   b. From the Network Overview, select the nodes you want to configure the QA probes on.

   c. Go to step 3.

   To launch the Probe Configuration form from the Interfaces Inventory

   a. Click **Inventory** → **Interfaces.**

   b. From the Interfaces inventory, select the interfaces you want to configure the QA probes on.

   c. Go to step 3.

   To launch the Probe Configuration form from the IP Addresses Inventory

   a. Click **Inventory** → **IP Addresses.**

   b. From the IP Addresses inventory, select the required IP Addresses you want to configure the QA probes on.

   c. Go to step 3.

3. Select **Actions** → **Quality Assurance** → **Probe Configuration.**

   The Probe Configuration form opens.

   The following icons are available in the Probe Configuration form:

Icons	Description
 Open	Opens a dialog box, where you can specify to open a file that has the probe configuration details. Browse button is provided to access the file.
 Close	Closes the Probe Configuration form without saving the current configuration.
 Save	Opens a dialog box, where you can specify to save the probe configuration details to a file in a specified directory.

Probe Configuration Form: Probe Definition Tab

You can use the **Probe Definition** tab to do the following tasks for the selected source and destination node:

- Create a new probe
- Create a probe using a pre-defined template
- Deploy the configured QA probes on the node
- Copy the probe definition

To create a new probe definition:

1. Launch the Probe Configuration form .
2. Enter the Source Node and Destination Node details.

   Source Node Details

Field Name	Description
Hostname	*Mandatory information* 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 *Configure Tenants* and *Configuring Security* in *HP Network Node Manager i Software Online Help: Help for Administrators*.
IP Address	Specify the IP address of the source node.

Field Name	Description
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 or PATH Echo services.
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	*Mandatory information* 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	*Mandatory information* Specify the name of the new probe.
VRF Name	Specify the VRF name.

Field Name	Description
Service	*Mandatory information* Select any of the following service types: ▪ ICMP Echo ▪ PATH Echo ▪ TCP Connect ▪ UDP ▪ UDP Echo ▪ VoIP ▪ HTTP ▪ DNS ▪ DHCP 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.
ToS	Specify the Type of Service.

4. Enter the following Duration Details:

Field Name	Description
Frequency	*Mandatory information* The frequency at which the probe must run the tests. Click this field to enter the hour, minute, and seconds.

Field Name	Description
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:

ICMP Details

In the Packet Size field, specify the packet size.

PATH Echo 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

Field Name	Description
Inter Packet Delay (Milliseconds)	Specify the inter packet delay in milliseconds
Codec Type	*Mandatory information* 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
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.

Probe Configuration Form: Template Definition Tab

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 .
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	*Mandatory information* Specify the name of the new probe template.
VRF Name	Specify the VRF name.

Field Name	Description
Service	*Mandatory information* Select one of the following service types: ▪ DNS ▪ HTTP ▪ HTTPS ▪ ICMP Echo ▪ Oracle ▪ TCP Connect ▪ UDP ▪ UDP Echo ▪ VoIP ▪ PATH Echo ▪ DHCP
ToS	Specify the Type of Service.

Duration Details

Field Name	Description
Frequency	*Mandatory information* 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.

Field Name	Description
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.

Field Name	Description
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	*Mandatory information* Specify the Oracle database user name.
Database Name	*Mandatory information* Specify the name of the database running on the target Oracle server.
Password	*Mandatory information* 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	*Mandatory information* Select the codec type.

PATH Echo Details

Specify the packet size.

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.

Deploying the 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. See Probe Definition tab for more information.
2. Click **Deploy** in the **Probe Definition** form.

To deploy the probes using the **Probe List** form:

1. Enter the probe definition details . See Probe Definition tab for more information.
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.

Probe Configuration Form: Deploy Status Tab

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: ▪ 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.

Field Name	Description
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	Refreshes the details.

Probe Configuration Form: Probe List Tab

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

   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.

Field Name	Description
Service	The service type of the QA probe can be any one of the following: ■ UDP Echo ■ ICMP Echo ■ UDP ■ TCP Connect ■ VoIP ■ HTTP ■ DNS ■ 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.

Probe Configuration Form: Template List Tab

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

   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: ▪ UDP Echo ▪ ICMP Echo ▪ PATH Echo ▪ UDP ▪ TCP Connect ▪ VoIP ▪ HTTP ▪ DNS ▪ DHCP
VRF Name	The name of the VRF.

Field Name	Description
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.

Probe Configuration Form: Preconfigured Probes Tab

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
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: ▪ Normal ▪ Warning ▪ Major ▪ Critical ▪ Unknown ▪ Disabled ▪ Not Polled ▪ No Status For more information on status, see QA Probe Status.
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.

Field Name	Description
Service	The service type of the QA probe. The valid service types are: ▪ 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 Real Time Line Graph.

Probe Configuration Form: Template Definition Tab

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 Configuration form .
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	*Mandatory information* Specify the name of the new probe template.
VRF Name	Specify the VRF name.

Field Name	Description
Service	*Mandatory information* Select any of the following service types: ▪ DNS ▪ HTTP ▪ HTTPS ▪ ICMP Echo ▪ Oracle ▪ TCP Connect ▪ UDP ▪ DHCP
ToS	Specify the Type of Service.

Duration Details

Field Name	Description
Frequency	*Mandatory information* 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	*Mandatory information* Specify the Oracle database user name.

Field Name	Description
Database Name	*Mandatory information* Specify the name of the database running on the target Oracle server.
Password	*Mandatory information* 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	*Mandatory information* 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.

Probe Configuration Form: Deploy Status Tab

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: ▪ 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.

Field Name	Description
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.

Probe Configuration Form: Preconfigured Probes Tab

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 Configuration form
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: ▪ Normal ▪ Warning ▪ Major ▪ Critical ▪ Unknown ▪ Disabled ▪ Not Polled ▪ No Status For more information on status, see QA Probe Status.
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.

Field Name	Description
Destination IP Address	The destination IP address for the probe.
Service	The service type for the probe. The valid service types are: ▪ 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 Real Time Line Graph.

NNM iSPI Performance for QA Site Configuration

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 Using Site Configuration Form.

QA Probes Association

[1]Some examples of network elements are routers and switches.
[2]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.

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.

  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.

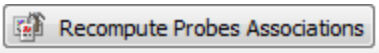
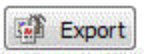
3. Select **Quality Assurance Configuration Console.**

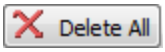
   The console opens.

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:

Icons Available in the Site Settings Toolbar	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 Probe Associations	Re-assigns the QA probes to the sites.
 Export	Exports the existing sites.
 Import	Imports sites from an XML file.
Icons Available in the Global Settings Panel	**Description**

Icons Available in the Site Settings Toolbar	Description
Enable Site Configuration	Enables to associate the configured sites to the probes.
Icons Available in the Configured Sites Tab	**Description**
 New	Adds a new site
 Clone	Clones (copies) the selected site
 Open	View an existing site
 Edit	Edits an existing site
 Delete	Deletes an existing 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 a New Site Using the Site Configuration Form

To add a new site:

1. Launch the Site Configuration form.
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.

[1]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.

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 NNMi administrator, you can create new tenants and security groups. See

[1] 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.

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 QApopulates 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 QAdoes 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.

Editing an Existing Site Using the Site Configuration Form

To edit an existing site:

1. Launch the Site Configuration form.
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. 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.

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.

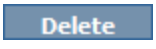
   NNMi provides a tenant named Default Tenant and assigns each newly discovered node to the Default Tenant and the Security Group attribute value configured for the Default Tenant. As an NNMi administrator, you can create new tenants and security groups. See *Configure Tenants* and *Configuring Security* in *HP Network Node Manager i Software Online Help: Help for Administrators*.

e. IP Address Range:

[1]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.

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 QApopulates 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 QAdoes 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 **Delete** to remove it from the Probe Name Patterns box.

You can click Delete All **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 **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 **Delete** to remove it from the VRF Wildcards box.

You can click Delete All **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.

Icons	Description
 Save and Close	Saves the site information and closes the Edit Site Configuration form.
 Clear	Clears the site information you have entered in the form.

5. Click  **Refresh** in the Configured Sites panel to view the changes.

Deleting an Existing Site Using the Site Configuration Form

To delete an existing site:

1. Launch the Site Configuration form .
2. Select a site in the **Configured Sites** panel and click  **Delete**.
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>
```

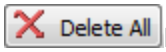
To synchronize the deletion of sites at all regional managers to the global manager:

```
nmsqasiteconfigutil -synchronize all
```

[1]Sites exported from the regional manager to the global manager are known as Remote Sites.

Deleting All the Existing Sites Using the Site Configuration Form

To delete all the existing sites:

1. Launch the Site Configuration form .
2. Click 

Delete All.
3. Click  **Refresh** in the **Configured Sites** panel to view the changes.

The QA probe associations for the sites are deleted automatically. You do not need to recompute the QA probe associations after deleting the sites.

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:

```
nmsqasiteconfigutil -synchronize all
```

[1]Sites exported from the regional manager to the global manager are known as Remote Sites.

Viewing an Existing Site Configuration Using the Site Configuration Form

To view a site configuration:

1. Launch the Site Configuration form .
2. Select a site in the **Configured Sites** panel and click  **Open**.

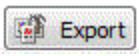
   The View Site Configuration Details form opens.

   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 a Site

To export the existing site configurations to an XML file:

1. Launch the Site Configuration form .
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 .
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.

Re-Computing Probes associated with a Site

NNM iSPI Performance for QA associates the QA probes with the respective sites during the configuration poll. However, if there are changes in the site configuration, the probes can be associated with the site by clicking the Recompute Probes Associations button.

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*

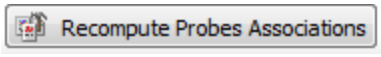
Also, you want to add the following VRF groups:

- 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 utility to associate the QA probes to the new or updated sites at once.

Use one of the following ways to recompute QA probe associations for the new or updated sites:

- Click 

Recompute Probes Associations on the Site Configuration form.
- Use the following command line utility:
  - **Linux:** `.$NnmInstallDir/bin/bin/nmsqasiteconfigutil.ovpl –u <username> –p <password> –recompute`
  - **Windows:** `%NnmInstallDir%\bin\nmsqasiteconfigutil.ovpl –u <username> –p`

```
<password> –recompute
```

By default, the `%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 -resetrecomputeQ
```

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

Cloning (Copying) Existing Site Configuration Using the Site Configuration Form

To clone the existing configuration for a selected site:

1. Launch the Site Configuration form .
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).

      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.

[1]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.

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.

[1] 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.

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 QApopulates 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 QAdoes 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 **Delete** to remove it from the Probe Name Patterns box.

You can click Delete All **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 **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 **Delete** to remove it from the VRF Wildcards box.

You can click Delete All **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.

NNM iSPI Performance for QA Discovery Filter Configuration

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. Using this feature, you can restrict to discover and monitor only a required set of probes in your network.

This feature 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.

The Discovery Filter Configuration 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.

Launching the Discovery Filter Configuration Form

To launch the discovery filter configuration:

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

   You must have administrator privileges.

2. Select **Configuration** workspace.

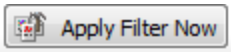
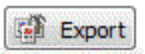
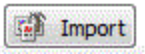
3. Select **Quality Assurance Configuration Console.**

   The console opens.

4. In the **Configuration** workspace, select **Probe Discovery Filters.**

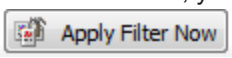
   The Discovery Filter Configuration form opens.

You can perform the following tasks from the Discovery Filter Configuration toolbar:

Icon	Description
 Close	Closes the Discovery Filter Configuration form without saving the current configuration.
 Save	Saves the current configuration.
 Save and Close	Saves the current configuration and closes the Discovery Filter Configuration form.
 Refresh	Retrieves the last saved discovery filter configuration from the database.
 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.
 Export	Exports the existing discovery filter configuration.
 Import	Imports discovery filter configuration from an XML file.

You can perform the following tasks from the Global Settings Panel:

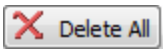
[1]Local QA probes are QA probes owned by the local sites.

Icon	Description
Enable Discovery Filters	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**.

The Registration panel provides details about the selected discovery filter:

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

You can perform the following tasks from the Configured Filters Tab:

Icon	Description
 New	Adds a new discovery filter.
 Edit	Edits an existing discovery filter.
 Delete	Deletes an existing discovery filter.
 Refresh	Retrieves the last saved discovery filter configuration from the database and displays the data in the Configured Filters panel.
 Delete All	Deletes all existing discovery filters.

Adding a New Discovery Filter Using the Discovery Filter Configuration Form

To add a new discovery filter:

1. Launch the Discovery Filter Configuration form.
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 **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 **Delete** to remove it from the Source IP Addresses box.

You can click Delete All **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 **Delete** to remove it from the Destination IP Addresses box.

You can click Delete All **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.

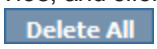
f. **Service**

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

Add

- **UDP Echo**
- ICMP Echo
- UDP
- TCP Connect
- VoIP
- **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.

Editing a Discovery Filter Using the Discovery Filter Configuration Form

To edit a discovery filter:

1. Launch the Discovery Filter Configuration form.
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:

   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 Delete to remove it from the Owner Names box.

You can click Delete All **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 **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 **Delete** to remove it from the Source IP Addresses box.

You can click Delete All **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 **Add.** You can add IPv4 and IPv6 addresses. Select a Destination IP address or IP address range and click Delete **Delete** to remove it from the Destination IP Addresses box.

You can click Delete All **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:

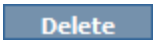
- For IPv4 addresses, you can use "**-**" (the character hyphen) when defining a range of IPv4 addresses.
- Specify the range in the ascending order. The range must be from a lower value to a higher value.
- For IPv4 addresses, use the wild card character "*" to specify IP addresses between 0 to 255.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

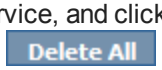
f. **Service**

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
- **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 an Existing Discovery Filter Using the Discovery Filter Configuration Form

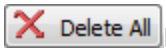
To delete an existing discovery filter:

1. Launch the Discovery Filter Configuration form.
2. Select a filter in the **Configured Filters** panel, and click  **Delete**.
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.

Deleting All Existing Discovery Filters Using the Discovery Filter Configuration Form

To delete all the existing discovery filters:

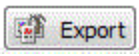
1. Launch the Discovery Filter Configuration form.
2. Click 

Delete All.
3. Click  **Refresh** in the **Configured Filters** panel to view the changes.

After you delete all discovery filters, the filtered probes are discovered in the next discovery cycle.

Exporting a Discovery Filter

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

1. Launch the Discovery Filter Configuration form.
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 Discovery Filters

To import discovery filter configurations from an XML file:

1. Launch the Discovery Filter Configuration form.
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\nmsqadiscofilter.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.

NNM iSPI Performance for QA Global Network Management Configuration

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* guide.

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 a new regional Manager.
 Open	Opens the Modify Regional Manager Configuration form of the selected Regional Manager.
 Delete	Deletes the selected regional manager.
 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.

Field Name	Description
Connection State	The Connection status can be one of the following: • Not Established • Connected

Creating a New Regional Manager

To create a new regional manager:

1. Launch the Global Network Management Configuration form.
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 a new regional manager connection.
 Open	Opens the Modify Regional Manager Connections form of the selected regional manager connection.
 Delete	Deletes the details of the selected regional manager connection.

Icon	Description
 Refresh	Refreshes and displays the last saved regional manager connection.

Adding a Regional Manager Connection

1. Launch the Global Network Management Configuration form.
2. Ensure that you enter the Name in the Create Regional Manager form.
3. Click  **New** in the **Connections** panel of the Create New 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), you must enter the port number for the HTTPS protocol.

      If you have not selected the Use Encryption (previous field), you must enter the port number for the HTTP protocol.

   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.
 Clear	Clears the regional manager connection information you have entered in the form.

Modifying a Regional Manager Connection

1. Launch the Global Network Management Configuration form.
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), you must enter the port number for the HTTPS protocol.

      If you have not selected the Use Encryption (previous field), you must enter the port number for the HTTP protocol.

   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.
 Clear	Clears the regional manager connection information you have entered in the form.

Editing an Existing Regional Manager

You can modify an existing regional manager and regional manager connections as well.

Editing an Existing Regional Manager by using the Modify Regional Manager Configuration Form

To modify a regional manager:

1. Launch the Global Network Management Configuration form.
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. Click the **Connections** tab.
6. You can perform the following actions:

Icon	Description
 New	Adds a new regional manager connection.
 Open	Opens the Modify Regional Manager Connections form of the selected regional manager connection.

Delete	Deletes the details of the selected regional manager connection.
Refresh	Refreshes the Regional Manager Connections panel and displays the last saved regional manager connection.

Editing an Existing Regional Manager Connection Using the Modify Regional Manager Connection Form

To modify a regional manager connection:

1. Launch the Global Network Management Configuration form.
2. Select the regional manager you want to modify and click **Open.**

   The Modify Regional Manager Configuration form opens.
3. Select the regional manager connection you want to modify and click **Open** in the Connections panel.

   The Modify Regional Manager Connection form opens.

4. You can modify the following information:

Field Name	Description
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 selected HTTPS option in the NNMi management server, you must select the Use Encryption option. However, if you selected the HTTP option in NNMi management server, you must clear the Use Encryption option.
HTTP(S) Port	If you selected the Use Encryption (previous field), you must enter the port number of the HTTPS protocol. If you did not select the Use Encryption (previous field), you must enter the port number of the HTTP protocol.
User Name	Type a valid user name for the regional NNMi management server.
User Password	Type the password for the User Name.
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. You can perform 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.
 Clear	Clears the regional manager connection information you have entered in the form.

Deleting an Existing Regional Manager

Deleting an Existing Regional Manager Configuration Using Global Network Management Configuration Form

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:

1. Launch the Global Network Management Configuration form.
2. Select the regional manager you want to delete and click  **Delete.**
3. Click  **Refresh** to view the changes.

Deleting an Existing Regional Manager Connection Using Modify Regional Manager Configuration Form

If you delete a regional manager configuration, all the objects associated with the regional manager are also deleted.

To delete a regional manager connection:

1. Launch the Global Network Management Configuration form.
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.

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 group[1]
- View the entities based on the groups[2]
- Configure polling frequency[3]

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

[1]You 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.
[2]You can view the state of the entities based on the QA group.
[3]You 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.

- Destination Site
- Node Group Name

Grouping attributes for CBQoS 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

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

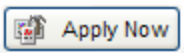
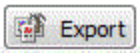
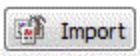
Launching the QA Groups Configuration Form

To launch the Configure a QA Group form:

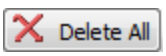
1. Log on to NNMi console using your user name and password.

   You must have administrator privileges.

2. From the workspace navigation panel, select **Configuration.**
3. Click **Quality Assurance Configuration Console.**
4. Select **QA Groups** from the Configuration workspace.
5. You can perform the following actions from the QA Groups configuration toolbar:

Icon	Description
 Close	Closes the QA Groups configuration form without saving the current configuration.
 Refresh	Retrieves the last saved configuration from the database and displays that data.
 Apply Now	Applies the configured QA Groups.
 Export	Exports the existing configured QA Groups.
 Import	Imports the existing configured QA Groups.

6. You can perform the following actions from the configured QA Groups tab:

Icon	Description
 Add	Adds a new QA Group.
 Edit	Edits an existing configured QA Group.
 Delete	Deletes an existing configured QA Group.
 Refresh	Retrieves the last saved configuration from the database and displays that data.
 Delete All	Deletes all the existing configured QA Groups.
Select all	Selects all the existing QA Groups.

Adding a New QA Group

To add a new QA Group:

1. Launch the QA Groups configuration form.
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	A brief description of the QA Group. For example, you can mention "Probes for VoIP", if you want to group all VoIP probes. **Note:** Do not use the & and < characters in the description.
Type	The type of the QA Group. The valid QA Group types are QA Probes, Ping Latency, and CBQoS. Select a type for the new QA group before you continue creating the QA group filters.
Tenant	The tenant name to which the QA group belongs to. 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 *Configure Tenants and Configuring Security* in *HP Network Node Manager i Software Online Help: Help for Administrators*.

Field Name	Description
Polling Interval	The applicable polling interval for all the members of the QA group, in seconds. ■ For CBQoS 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. If a CBQoS entity is a member of multiple QA groups, then it's polling frequency is that of the QA group with the lowest polling interval. 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. To configure the polling frequency of the QA Probes/CBQoS entities that are not part of any QA group, see Polling Configuration. **Note:** For QoS interfaces, it is recommended that you do not use a polling interval of less than 1 minute. For probes, you cannot use a polling interval of less than 1 minute.
Filter Editor	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. 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.

[1]Adds the current Boolean Operator to the beginning of the selected Boolean Operator within the Filter String.
[2]Adds the current Boolean Operator to the end of the selected Boolean Operator within the Filter String.
[3]Replaces the selected Boolean Operator with the current Boolean Operator within the Filter String.
[4]Adds the current condition (Attribute, Operator, and Value) to the beginning of the conditions already added to the selected boolean operator.
[5]Adds the current condition (Attribute, Operator, and Value) to the end of the conditions already added to the selected boolean operator.
[6]Replaces 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)
```

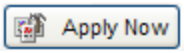
To add the Filter Editor expression above, after you are in the Filter Editor section, follow these steps:

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 the 

Apply Now in the QA Groups panel, or during the next discovery cycle of the nodes.

Editing the Existing QA Groups

To edit the existing QA Groups:

1. Launch the QA Groups configuration form.
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. **Note:** Do not use the & and < characters in the description.
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 *Configure Tenants and Configuring Security* in *HP Network Node Manager i Software Online Help: Help for Administrators*.
Polling Interval	The applicable polling interval for all the members of the QA group, in seconds. For QA probes: ▪ 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: ▪ If the value remains zero, the polling interval of the QA Group is the default value, which is 300 seconds.

Field Name	Description
	▪ 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 Polling Configuration.

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] b
oolean 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.

[1]Adds the current Boolean Operator to the beginning of the selected Boolean Operator within the Filter String.
[2]Adds the current Boolean Operator to the end of the selected Boolean Operator within the Filter String.
[3]Replaces the selected Boolean Operator with the current Boolean Operator within the Filter String.

To edit a condition: Use the rule components to insert[1], append[2], and replace[3] a condition.

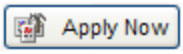
Component	Description
Attribute	The attribute on which you want NNM iSPI Performance for QA to filter the probes. The listed attributes depend on the type of the QA Group selected.
Operator	The operator that establishes the relationship between the Attribute and Value.
Value	The value that completes 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.**

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.**

[1]Adds the current condition (Attribute, Operator, and Value) to the beginning of the conditions already added to the selected boolean operator.
[2]Adds the current condition (Attribute, Operator, and Value) to the end of the conditions already added to the selected boolean operator.
[3]Replaces the selected condition with the current condition within the Filter String.

Deleting an Existing QA Group

To delete an existing QA Group:

1. Launch the QA Groups configuration form.
2. Select the QA Group that you want to delete, and click  **Delete** in the **Configured QA Groups** tab.
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:`$NnmInstallDir/bin/ nmsqacustomgrouputil.ovpl -u <username> -p <password> -delete -g <QA group name>`

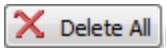
Windows:`%NnmInstallDir%\bin\nmsqacustomgrouputil.ovpl -u <username> -p <password> -delete -g <QA group name>`

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.

Deleting all Existing QA Groups

To delete all the existing QA Groups:

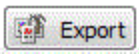
1. Launch the QA Groups Configuration form.
2. Click 

Delete All in the **Configured QA Groups** tab.
3. Click  **Refresh** in the Configured QA Groups tab to view the changes.

If you delete the QA Groups, 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.

Exporting the QA Group Configurations

To export the QA probes associated with a QA group to an XML file:

1. Launch the QA Group Configuration form.
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
`nmsqacustomgrouputil.ovpl -u <username> -p <password> -export <filename to export the QA group configurations>`	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 the QA Group Configurations

To import QA group configurations from an XML file:

1. Launch the QA Group Configuration form.
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 Filters

The various operators that are used with the attributes in defining the QA Group filters are given below:

<table>
<tr><th>Operator</th><th>Description</th></tr>
<tr><td>=</td><td>Finds all values equal to the value specified. For example, <code>Node Group = Cisco</code> finds all the node groups with the name Cisco.</td></tr>
<tr><td>!=</td><td>Finds all values not equal to the value specified. For example, <code>Node Group != Cisco</code> finds all the node groups other than Cisco.</td></tr>
<tr><td>like</td><td>Finds matches using wild card characters. For example, <code>Interface Description (ifDescr) like Fa 0/1</code> finds all interface names that begin with Fa 0/1.</td></tr>
<tr><td>Not like</td><td>Finds all that do not have the values specified (using wild card strings). For example, <code>Interface Description (ifDescr) not like Fa 0/1</code> finds all interface names that do not begin with Fa 0/1.</td></tr>
<tr><td>In</td><td>Finds a match to at least one of the values specified. For example:<table><tr><th>Attribute</th><th>Value</th></tr><tr><td>Policy Name</td><td>P1
P2</td></tr></table>Finds all policy names that are P1 or P2.
Note: You must enter each value in a separate line.</td></tr>
<tr><td>Not in</td><td>Finds all values except those included in the list of values. For example:<table><tr><th>Attribute</th><th>Value</th></tr><tr><td>Policy Name</td><td>P1
P2</td></tr></table>finds all policy names other than P1 and P2.
Note: You must enter each value in a separate line.</td></tr>
<tr><td>Between</td><td>Finds all values equal to and between the two values specified. Use this operator only on attributes that have numeric values.</td></tr>
<tr><td>Not between</td><td>Finds all values except those between the two values specified. Use this operator only on attributes that have numeric values.</td></tr>
</table>

Operator	Description
Range	Finds all values within the specified IP address range. You can specify the range in one of the following formats: • Wild card characters in place of octets For example: ▪ 192.168.*.* • Ranges of numbers in place of octets For example: ▪ 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**

Ping Latency Pair Configuration

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.

[1] 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.

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 `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 segments of a router-node pair definition:

Source Details

The Source Details segment includes the following entities:

Entity	Description
Host Name	*This is a mandatory entity.* 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

Details	Description
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: Asterisk (*) represents any string Question mark (?) represents a single character
Dest_ IPAddress	*This is a mandatory entity.* 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.

Configure Ping Pairs in the PingPair.conf File

To configure the ping latency pairs, 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 315.
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 (see Table: Default Attributes of Each Ping Request).

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 315.

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

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

Configure 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. Table: Default Attributes of Each Ping Request lists the default attribute values. To change the default attribute values, you must edit the `PingPairPoll.conf` file.

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 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**

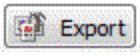
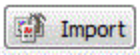
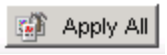
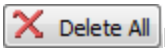
NNM iSPI Performance for QA Threshold Configuration for Ping Latency Pairs

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. Perform the configuration task of your choice (see table).

Tasks for Ping Pair Threshold Configuration

Task	How
 Add	Launch the Ping Pair - Add Threshold Configuration form to add a new threshold.
 Edit	Select an existing ping pair and launch the Ping Pair - Edit Threshold Configuration form to edit the threshold.
 Export	Exports the existing threshold configurations.
 Import	Imports the existing threshold configurations.
 Apply All	Applies all the threshold configurations.
 Close	Closes the Threshold Configuration form without saving the current configuration.
Refresh	Click  **Refresh** to refresh the list of thresholds.
Delete	Select an existing ping pair and click  **Delete** to delete the threshold.
Delete All	Click  **Delete All** to delete all existing thresholds.

Add a New Ping Pair Threshold

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.**

Add a New Threshold Setting

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.

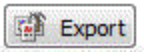
Edit an Existing Ping Pair Threshold

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 (see "Add a New Threshold Setting" on page 323). You can add more than one threshold setting.
4. Click Delete  **Delete** to delete a threshold setting.
5. Click  **Save and Close**.

Exporting the Ping Latency Pair Threshold Configurations

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:

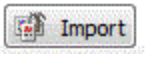
Linux:`$NnmDataDir/log/qa/qa.log`

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.

Polling Configuration

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 five 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: 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.

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.

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.
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.

Probe-Based Threshold Configuration

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.

[1]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.

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

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.

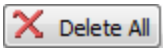
5. Click **Actions→ Quality Assurance → Configure Threshold.**
   - If you are configuring a new threshold value for the selected QA probes, the Add Threshold Configuration form opens.
   - If a threshold value already exists for the selected QA probes, the Edit Threshold Configuration form opens.
   - 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:

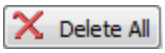
Icon	Description
 Close	Closes the Threshold Configuration form without saving the current configuration.
 Save and Close	Saves the current configuration and closes the Threshold Configuration form.

[1]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.

7. You can do the following in the Threshold Settings Tab:

Icon	Description
 New	Adds a new threshold for the QA probes.
 Edit	Edits an existing threshold for the QA probes.
 Delete	Deletes an existing threshold of the QA probes.
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data.
 Delete All	Deletes all the existing thresholds of the QA probes.

8. You can do the following in the Baseline Settings Tab:

Icon	Description
 New	Adds a baseline setting for the QA probes.
 Edit	Edits an existing baseline setting for the QA probes.
 Delete	Deletes an existing 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 existing baseline settings of the QA probes.

Adding New Threshold Settings Using the Threshold Configuration Form

To add a new threshold:

1. Make sure that you selected the Source Site, and Service in the Add 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. To see the metrics for each service type, click here.

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	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 Round Trip Time (RTT) you must generate an

Field Name	Description
	incident when the RTT is 150 and clear the incident when the RTT value comes down to 100. Set the following values for the threshold: ▪ High Value: `150` ▪ High Value Rearm: `100` This value enables you to be aware when a network 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	Enter the low value rearm for the threshold. For Packet Loss metric, enter the Low Rearm Value in percentage. 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. The low value rearm must be greater than the low value. **Example** 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. Set the following values for the threshold: ▪ Low Value: `3` ▪ Low Value Rearm: `4.5` This value enables you to be aware when a network performance problem starts to improve.

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	Designate the minimum time within which the metric value must remain in the High range. 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. You define the high threshold value in the High Value field. 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..
High Duration Window	Designate the window of time within which the High Duration criteria must be met. To enable this setting, the value must be: ▪ greater than 0 (zero) ▪ the same as or greater than the High 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. 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.

The following fields appear if you selected the Type as Time-Based and the metric as MOS:

Low Duration	Designate the minimum time within which the metric value must remain in the Low range. 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. You define the low threshold value in the Low Value field. The polling interval should be less than or equal to the Low Duration.
Low Duration Window	Designate the window of time within which the Low Duration criteria must be met. 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. To enable this setting, the value must be: ▪ greater than 0 (zero) ▪ the same as or greater than the Low Duration value The NNM iSPI Performance for QAuses 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.

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.

Icons	Description
 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 an Existing Threshold Setting Using the Threshold Configuration Form

To edit an existing threshold setting:

1. Specify all the mandatory fields in Edit Threshold Configuration form.

   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	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 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.

[1]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.

Field Name	Description
	Set the following values for the threshold: ▪ High Value: `150` ▪ High Value Rearm: `100` This value enables you to be aware when a network 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	Enter the low value rearm for the threshold. For Packet Loss metric, enter the Low Rearm Value in percentage. 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. The low value rearm must be greater than the low value. **Example** 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. Set the following values for the threshold: ▪ Low Value: `3` ▪ Low Value Rearm: `4.5` This value enables you to be aware when a network performance problem starts to improve.

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	Designate the minimum time within which the metric value must remain in the High range. 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. You define the high threshold value in the High Value field. 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..
High Duration Window	Designate the window of time within which the High Duration criteria must be met. To enable this setting, the value must be: ▪ greater than 0 (zero) ▪ the same as or greater than the High 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. 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.

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	Designate the minimum time within which the metric value must remain in the Low range. 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. You define the low threshold value in the Low Value field. The polling interval should be less than or equal to the Low Duration.
Low Duration Window	Designate the window of time within which the Low Duration

	criteria must be met. 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. To enable this setting, the value must be: ▪ greater than 0 (zero) ▪ the same as or greater than the Low Duration value The NNM iSPI Performance for QAuses 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.

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.

Adding New Baseline Settings Using the Threshold Configuration Form

To add a new baseline setting configuration:

1. Make sure that you selected the Source Site, and Service in the Add Threshold Configuration form .

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: ▪ 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	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.

Field Name	Description
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.
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 QAuses 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.

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 Using the Threshold Configuration Form

To edit a baseline setting configuration:

1. Make sure that you selected the Source Site, and Service in the Edit Threshold Configuration form 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.

Field Name	Description
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.
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 QAuses 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 an Existing Threshold of QA Probes Using the Edit Threshold Configuration Form

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**.
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: TestUp[1], RttThresholdStateHigh,TwoWayPktLossThresholdStateHigh

After Deleting the Threshold(s) Configured for the QA Probe:

QA Probe Status : Normal

Threshold State: Threshold Not Set

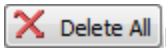
If the QA probe is associated with a site the Threshold State is updated based on the threshold configured for the site.

Conclusion: TestUp[2]

[1]When both Administrative and Operational states are up.
[2]When both Administrative and Operational states are up.

Deleting All Existing Thresholds of QA Probes Using the Edit Threshold Configuration Form

To delete all the existing thresholds of QA probes:

1. Launch the Configure Threshold form .
2. Click 

Delete All.
3. Click  **Refresh** in the Threshold Settings panel to view the changes.

The following changes occur after deleting a probe based threshold configuration:

The thresholds configured for the QA probes are deleted and the threshold state is set to Threshold Not Set for the QA probe. The QA Probe status is set to the most severe status. If the QA probe is associated with a site, the threshold state of the site is associated with the QA probe. The incidents and conclusions are updated accordingly.

Example 1

Consider the following scenario:

Before Deleting all the Thresholds 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 all the Thresholds 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 all the Thresholds Configured for the QA Probe

QA Probe Status : Major

Threshold State: High

Conclusion: TestUp[1], RttThresholdStateHigh,TwoWayPktLossThresholdStateHigh

After Deleting all the Thresholds Configured for the QA Probe:

QA Probe Status : Normal

Threshold State: Threshold Not Set

If the QA probe is associated with a site the Threshold State is updated based on the threshold configured for the site.

Conclusion: TestUp[2]

[1]When both Administrative and Operational states are up.
[2]When both Administrative and Operational states are up.

Launching the Probe-Specific Threshold Configuration Form

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 **Probes** >**Probe Specific Threshold**.

   The Probe Specific Threshold form opens.

   For more information, see the topic Configure threshold for QA Probes.

   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: ■ **UDP Echo** ■ **ICMP Echo** ■ **UDP Echo** ■ **TCP Connect** ■ **VoIP**
Owner	The name of the QA probe's owner.

Probes with Specific Thresholds, continued

Attribute Name	Description
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	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

NNM iSPI Performance for QA Probe Threshold Configuration (Sites and QA Groups)

Launching the Threshold Configuration Form

To launch the QA Probe 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.

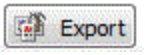
3. Select **Quality Assurance Configuration Console**.
   The console opens.

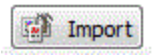
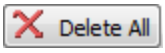
4. In the **Configuration** workspace, select **Probes** > **Sites/QA Group.**

   The Threshold Configuration form opens.

You can perform the following tasks using the Threshold Configuration form:

Any changes made to the threshold settings are applied to the poller immediately.

Icons Available in the Threshold Configuration Toolbar	Description
 Close	Closes the Threshold Configuration form without saving the current configuration
 Save	Saves the current configuration.
 Save and Close	Saves the current configuration and closes the Threshold Configuration form
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data in the Threshold Configuration form
 Export	Exports the existing threshold configurations • Site • QA Group

Icons Available in the Threshold Configuration Toolbar	Description
 Import	Imports the existing threshold configurations • Site • QA Group
Icons Available in the Global Settings Panel	**Description**
Enable	Enables the site wide threshold configuration
Icons Available in the Site Wide Configuration Panel	**Description**
 New	Adds a new threshold configuration • Site • QA Group
 Edit	Edits an existing threshold configuration • Site • QA Group
 Delete	Deletes an existing threshold configuration: • Site • QA Group
 Refresh	Retrieves the last saved data from the database and displays the data in the Site Wide Configuration panel
 Delete All	Deletes all the existing thresholds • Site • QA Group

NNM iSPI Performance for QA Threshold Configuration for Sites

NNM iSPI Performance for QA thresholds enable you to track the health and performance of the network elements[1] in a network.

You can establish thresholds for the probes associated with sites. You can configure these thresholds to create an incident whenever the network performance measurement assigned to the site breaches the threshold.

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)

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.

You can see the contents of the topic Probe Specific Threshold Configuration to override thresholds of probes specific to a site.

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

[1]Some examples of network elements are routers and switches.

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 New Threshold Configuration

To add a new threshold configuration:

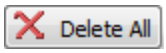
1. Launch the Threshold Configuration form .
2. Click  **New** in the **Threshold Configuration** panel.

   The Add Threshold Configuration form opens.
3. Select **Site** in Threshold Type field.
4. Specify the following information in the **Threshold Configuration** panel:

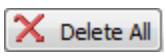
Field Name	Description
Threshold Type	In the Threshold Type, select **Site Based**.
Order	Specify a numeric value. NNM iSPI Performance for QA checks the configuration settings in the order you define (lowest number first)
Source Site	Select the name of the source site. This field is mandatory.
Destination 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: ▪ UDP Echo ▪ ICMP Echo ▪ UDP ▪ TCP Connect ▪ HTTP ▪ VoIP ▪ DNS ▪ DHCP

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.

Icons Available in the Threshold Settings Tab	Description
 New	Adds a new threshold for the site
 Edit	Edits the threshold for the site
 Delete	Deletes the selected threshold for the site
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data
 Delete All	Deletes all the threshold configured for the site

6. You can perform the following tasks when you click on the **Baseline Settings** tab.

Icons Available in the Baseline Settings Tab	Description
 New	Adds a new baseline setting for the site
 Edit	Edits the baseline setting 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 New Threshold Settings Using the Threshold Configuration Form

To add a new threshold:

1. Make sure that you selected the Source Site, and Service in the Add 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. To see the metrics for each service type, click here.

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	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 Round Trip Time (RTT) you must generate an

Field Name	Description
	incident when the RTT is 150 and clear the incident when the RTT value comes down to 100. Set the following values for the threshold: ▪ High Value: `150` ▪ High Value Rearm: `100` This value enables you to be aware when a network 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	Enter the low value rearm for the threshold. For Packet Loss metric, enter the Low Rearm Value in percentage. 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. The low value rearm must be greater than the low value. **Example** 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. Set the following values for the threshold: ▪ Low Value: `3` ▪ Low Value Rearm: `4.5` This value enables you to be aware when a network performance problem starts to improve.

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	Designate the minimum time within which the metric value must remain in the High range. 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. You define the high threshold value in the High Value field. 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..
High Duration Window	Designate the window of time within which the High Duration criteria must be met. To enable this setting, the value must be: ▪ greater than 0 (zero) ▪ the same as or greater than the High 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. 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.

The following fields appear if you selected the Type as Time-Based and the metric as MOS:

Low Duration	Designate the minimum time within which the metric value must remain in the Low range. 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. You define the low threshold value in the Low Value field. The polling interval should be less than or equal to the Low Duration.
Low Duration Window	Designate the window of time within which the Low Duration criteria must be met. 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. To enable this setting, the value must be: ▪ greater than 0 (zero) ▪ the same as or greater than the Low Duration value The NNM iSPI Performance for QAuses 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.

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.

Icons	Description
 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`

Adding New Baseline Settings Using the Threshold Configuration Form

To add a new baseline setting configuration:

1. Make sure that you selected the Source Site, and Service in the Add Threshold Configuration form .

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: ▪ 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	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.

Field Name	Description
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.
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 QAuses 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.

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 QA Probe Threshold Configuration form .
2. Select the threshold configuration settings to modify, and click  **Edit**.

   The Edit Threshold Configuration form opens.

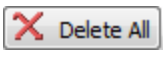
   When you edit a QA Group threshold configuration setting, NNM iSPI Performance for QA enables you to edit only the metric values, and does not enables you to edit the following fields:

   - Threshold Type
   - Order
   - Source Site
   - Destination Site
   - Service

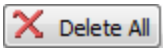
   If you want to edit the above mentioned fields, delete the existing configuration settings and configure a new threshold setting, based on your requirements.
3. Follow the steps in Editing an Existing Threshold to modify the metric values.

   You can view two tabs; **Threshold Settings** and **Baseline Settings**.

You can view the following options when you click on the **Threshold Settings** tab.

Icons Available in the Threshold Settings Tab	Description
 New	Adds a new threshold for the site
 Edit	Edits the selected threshold for the site
 Delete	Deletes the selected threshold for the site
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data
 Delete All	Deletes all the threshold configured for the site

You can view the following options when you click on the **Baseline Settings** tab:

Icons Available in the Baseline Settings Tab	Description
 New	Adds a new baseline deviation setting for the site
 Edit	Edits the baseline deviation setting for the site
 Delete	Deletes the selected baseline deviation settings 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 an Existing Threshold Setting Using the Threshold Configuration Form

To edit an existing threshold setting:

1. Specify all the mandatory fields in Edit Threshold Configuration form.

   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	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 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.

[1]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.

Field Name	Description
	Set the following values for the threshold: ▪ High Value: `150` ▪ High Value Rearm: `100` This value enables you to be aware when a network 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	Enter the low value rearm for the threshold. For Packet Loss metric, enter the Low Rearm Value in percentage. 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. The low value rearm must be greater than the low value. **Example** 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. Set the following values for the threshold: ▪ Low Value: `3` ▪ Low Value Rearm: `4.5` This value enables you to be aware when a network performance problem starts to improve.

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	Designate the minimum time within which the metric value must remain in the High range. 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. You define the high threshold value in the High Value field. 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..
High Duration Window	Designate the window of time within which the High Duration criteria must be met. To enable this setting, the value must be: ▪ greater than 0 (zero) ▪ the same as or greater than the High 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. 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.

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	Designate the minimum time within which the metric value must remain in the Low range. 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. You define the low threshold value in the Low Value field. The polling interval should be less than or equal to the Low Duration.
Low Duration Window	Designate the window of time within which the Low Duration

	criteria must be met. 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. To enable this setting, the value must be: ▪ greater than 0 (zero) ▪ the same as or greater than the Low Duration value The NNM iSPI Performance for QAuses 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.

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 Using the Threshold Configuration Form

To edit a baseline setting configuration:

1. Make sure that you selected the Source Site, and Service in the Edit Threshold Configuration form 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.

Field Name	Description
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.
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 QAuses 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 an Existing Threshold Using the Threshold Configuration Form

To delete an existing threshold:

1. Launch the QA Probe Threshold Configuration form .
2. Select a threshold in the **Threshold Settings** panel and click  **Delete**.
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: TestUp[1], RttThresholdStateHigh,TwoWayPktLossThresholdStateHigh

Deleting the Threshold(s) Configured for the Site:

QA Probe Status : Normal

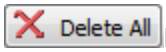
Threshold State: Threshold Not Set

Conclusion: TestUp[2]

[1]When both Administrative and Operational states are up.
[2]When both Administrative and Operational states are up.

Deleting All Existing Thresholds Using the Threshold Configuration Form

To delete all the existing thresholds:

1. Launch the QA Probe Threshold Configuration form .
2. Click 

Delete All.
3. Click  **Refresh** in the Threshold Settings panel to view the changes.

The following changes occur after deleting a site based threshold configuration:

The thresholds configured for the site is deleted and the threshold state is set to Threshold Not Set for the probes in the site for which you have not configured a probe based threshold configuration. The Probe status of the QA 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 all the Thresholds 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 all the Thresholds 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 of 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 all the Thresholds Configured for the Site

QA Probe Status : Major

Threshold State: High

Conclusion: TestUp[1], RttThresholdStateHigh,TwoWayPktLossThresholdStateHigh

After Deleting all the Thresholds Configured for the Site

QA Probe Status : Normal

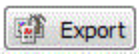
Threshold State: Threshold Not Set

Conclusion: TestUp[2]

[1]When both Administrative and Operational states are up.
[2]When both Administrative and Operational states are up.

Exporting a Threshold

To export the existing threshold configurations to an XML file:

1. Launch the QA Probe 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\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>`

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 QA Probe 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\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.

NNM iSPI Performance for QA Threshold Configuration 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 New QA Group Threshold Settings

To add a new QA Group threshold:

1. Launch the Threshold Configuration Form
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: • UDP Echo • ICMP Echo • UDP • TCP Connect • VoIP • HTTP • DNS

You can view the two tabs; Threshold Settings and Baseline Settings.

3. You can perform the following tasks when you click on the **Threshold Settings** tab.

Icons Available in the Threshold Settings Tab	Description
 New	Creates a new QA Groups threshold

Icons Available in the Threshold Settings Tab	Description
Edit	Edits an existing QA Groups threshold
Delete	Deletes an existing QA Groups threshold
Refresh	Retrieves the last saved threshold configuration from the database and displays the data
Delete All	Deletes all existing QA Groups thresholds

4. You can perform the following tasks when you click on the **Baseline Settings** tab.

Icons Available in the Baseline Settings Tab	Description
New	Creates a new QA Group threshold for baseline setting
Edit	Edits / overrides an existing QA Group threshold for baseline settings
Delete	Deletes an existing QA Group threshold for baseline settings
Refresh	Retrieves the last saved threshold configuration from the database and displays the data
Delete All	Deletes all existing QA Group thresholds for baseline settings

Creating New QA Group for QA Probe Threshold Setting

To add a new threshold:

1. Specify all the mandatory fields in the Adding New QA Groups Threshold Settings
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. To see the metrics for each service type, click here.

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	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 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.

Field Name	Description
	Set the following values for the threshold: ▪ High Value: `150` ▪ High Value Rearm: `100` This value enables you to be aware when a network 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	Enter the low value rearm for the threshold. For Packet Loss metric, enter the Low Rearm Value in percentage. 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. The low value rearm must be greater than the low value. **Example** 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. Set the following values for the threshold: ▪ Low Value: `3` ▪ Low Value Rearm: `4.5` This value enables you to be aware when a network performance problem starts to improve.

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	Designate the minimum time within which the metric value must remain in the High range. 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. You define the high threshold value in the High Value field. 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..
High Duration Window	Designate the window of time within which the High Duration criteria must be met. To enable this setting, the value must be: ▪ greater than 0 (zero) ▪ the same as or greater than the High 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. 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.

The following fields appear if you have selected the Type as Time-Based and the metric as MOS:

Low Duration	Designate the minimum time within which the metric value must remain in the Low range. 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. You define the low threshold value in the Low Value field. The polling interval should be less than or equal to the Low Duration.
Low Duration Window	Designate the window of time within which the Low

	Duration criteria must be met. 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. To enable this setting, the value must be: ▪ greater than 0 (zero) ▪ the same as or greater than the Low Duration value The NNM iSPI Performance for QAuses 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.

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 New QA Group Baseline Threshold Settings

To add a new baseline setting configuration:

1. Specify all the mandatory fields in the Adding New 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: ▪ 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	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.

Field Name	Description
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.
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 QAuses 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.

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 the QA Group Threshold Settings

To edit the QA Group threshold settings:

1. Launch the QA Probe Threshold Configuration Form
2. Select the threshold configuration settings to modify, and click  **Edit** in the Threshold Configuration form panel. The edit threshold configuration form opens.

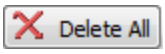
   When you edit the QA Group threshold configuration settings, NNM iSPI Performance for QA enables you to edit only the metric values, and does not enables you to edit the following fields:

   - Threshold type
   - Order
   - QA Group
   - Service

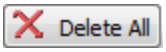
   If you want to edit the above mentioned fields, delete the existing configuration settings and configure a new threshold setting, based on your requirements.
3. Follow the steps in Editing an Existing Threshold to modify the metric values.

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 Available in the Threshold Settings Tab	Description
 New	Creates a new QA Group threshold
 Edit	Edits an existing QA Group threshold
 Delete	Deletes an existing QA Group threshold
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data
 Delete All	Deletes all existing QA Group thresholds

4. You can perform the following tasks when you click on the **Baseline Settings** tab.

Icons Available in the Baseline Settings Tab	Description
 New	Creates a new QA Group baseline threshold setting
 Edit	Edits / overrides an existing QA Group baseline threshold settings
 Delete	Deletes an existing QA Group baseline threshold settings
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data
 Delete All	Deletes all existing QA Group baseline threshold settings

Editing an Existing QA Group Threshold Setting

To edit an existing threshold setting:

1. Specify all the mandatory fields in Editing the 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	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 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. Set the following values for the threshold: ▪ High Value: `150` ▪ High Value Rearm: `100` This value enables you to be aware when a network performance problem starts to improve.

Field Name	Description
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 metric, enter the Low Rearm Value in percentage. 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. The low value rearm must be greater than the low value. **Example** 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. Set the following values for the threshold: ▪ Low Value: 3 ▪ Low Value Rearm: 4.5 This value enables you to be aware when a network performance problem starts to improve.

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	Designate the minimum time within which the metric value must remain in the High range. 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. You define the high threshold value in the High Value field. 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..
High Duration Window	Designate the window of time within which the High Duration criteria must be met. To enable this setting, the value must be: ▪ greater than 0 (zero) ▪ the same as or greater than the High 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. 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.

The following fields appear if you have selected the Type as Time-Based and the metric as MOS:

Low Duration	Designate the minimum time within which the metric value must remain in the Low range. 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. You define the low threshold value in the Low Value field. The polling interval should be less than or equal to the Low Duration.
Low Duration Window	Designate the window of time within which the Low Duration criteria must be met.

	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. To enable this setting, the value must be: ▪ greater than 0 (zero) ▪ the same as or greater than the Low Duration value The NNM iSPI Performance for QAuses 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. 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 the QA Group Baseline Threshold Settings

To edit the threshold for baseline settings:

1. Launch the QA Probe Threshold Configuration form.
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 in Editing the QA Group Baseline Threshold Setting, to modify the metric values.

Editing the QA Group for QA Probe Baseline Threshold Settings

To edit the threshold for baseline settings:

1. Specify all the mandatory fields in the Editing the 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	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 QAuses 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:

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 an Existing QA Group for QA Probe Threshold Setting

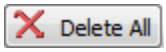
To delete an existing QA Group for QA Probe threshold:

1. Launch the QA Probe Threshold Configuration Form.
2. Select one or more configured QA Group threshold settings in the **Threshold Settings** panel and click  **Delete**.
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 all Existing QA Group Thresholds

To delete all existing QA Group for QA probe thresholds:

1. Launch the QA Probe Threshold Configuration Form.
2. Click 

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 an Existing QA Group for QA Probe Baseline Threshold

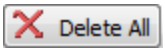
To delete an existing QA Group for QA Probe baseline threshold:

1. Launch the QA Probe Threshold Configuration Form.
2. Select **Baseline Settings** tab.
3. Select one or more threshold settings in the **Baseline Settings** panel, and Click  **Delete**
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.

Deleting all Existing QA Group for QA Probe Baseline Thresholds

To delete all existing QA Group for baseline thresholds:

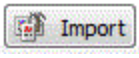
1. Launch the QA Probe Threshold Configuration Form.
2. Select **Baseline Settings** tab, and Click 

3. 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 the Existing QA Group Thresholds

To import the existing QA Group for QA Probe thresholds configurations from an XML file:

1. Launch the QA Probe Threshold Configuration Form.
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/nmsqathresholdconfigutil.ovpl –u <username> –p <password> –import –type qaprobe <filename>`

Windows:`%NnmInstallDir%\bin\nmsqathresholdconfigutil.ovpl –u <username> –p <password> –import –type qaprobe <filename>`

If the threshold import fails, check the following log files:

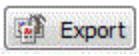
Linux: `$NnmDataDir/log/qa/qa.log`

Windows:`%NnmDataDir%\log\qa\qa.log`

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

Exporting the Existing QA Group Thresholds

To export the existing QA Group for QA Probe threshold configurations to an XML file:

1. Launch the QA Probe Threshold Configuration Form .
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/nmsqathresholdconfigutil.ovpl -u <username> -p <password> -export -type qaprobe <filename>`

Windows:`%NnmInstallDir%\bin\nmsqathresholdconfigutil.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.

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 information on incidents, see the topic QA Probes Form: Incidents Tab

NNM iSPI Performance for QA Quality of Service (QoS)

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

As the NNM iSPI Performance for QA administrator, you can perform the following tasks to monitor QoS interfaces:

- Create thresholds to track the health and performance of the QoS interfaces and nodes on your network.
- Create discovery filters to monitor only a required set of QoS elements enforced in a network environment.
- Create groups with QoS-managed nodes and interfaces

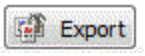
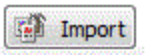
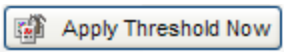
NNM iSPI Performance for QA supports Cisco CBQoS interfaces and nodes. NNM iSPI Performance for QA uses the CISCO-CLASS-BASED-QOS-MIB to collect the CBQoS performance data.

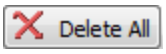
Chapter 2: Configuring QoS Thresholds

You can configure thresholds for QoS managed network elements and QA Group (QoS Probes), using the NNM iSPI Performance for QAfor QoS Threshold configuration.

To launch the QoS threshold configuration form:

1. Launch the Quality Assurance Configuration Console.
   a. From the workspace navigation panel, select the **Configuration** workspace.
   b. Double-click **Quality Assurance Configuration Console**.
2. In the Quality Assurance Configuration Console, go to the Workspaces navigation panel, and then expand **Threshold Configuration**.
3. Double-click **QoS.** The QoS Threshold Configuration form opens.
4. Do one of the following:
   - To configure a new threshold, click  **New** and continue.
   - To edit an existing threshold, click  **Edit** and continue.
5. Select **QoS Threshold** from the Configuration workspace.
6. You can perform the following tasks using the QoS Threshold Configuration Toolbar:

Icon	Description
 Close	Closes the Threshold Configuration form without saving the current configuration.
 Refresh	Retrieves the last saved configurations from the database and displays the data.
 Export	Exports the existing threshold configurations.
 Import	Imports the existing threshold configurations.
 Apply Threshold Now	Applies the threshold for all configured QA Groups.

Icon	Description
 Add	Adds new threshold settings • QoS • QA Group
 Edit	Edits an existing threshold settings • QoS • QA Group
 Delete	Deletes an existing threshold settings • QoS • QA Group
 Refresh	Retrieves the last saved configuration settings from the database and displays the data.
 Delete all	Deletes all existing threshold settings. • QoS • QA Group

NNM iSPI Performance for QA: QoS Threshold Configuration

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 Policy[1]
- 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.

[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.

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.

Adding New QoS Threshold Using the Add Threshold Configuration Form

To add a new QoS threshold:

1. Launch the QoS Threshold configuration form.

   The Add 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	Specify the name you want to assign to the threshold. Threshold names are case sensitive. That is `ThresholdA` and `thresholdA` are considered two different thresholds. Threshold names must be unique. Also, it is recommended to use unique threshold names across the QoS elements in a GNM environment. Use only alphanumeric characters to define threshold names. Threshold names cannot contain special characters.
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. 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. For example, you configured threshold T1 based on the class called DefaultClass and T2 based on the node group

Field Name	Description
	Routers. The ordering number for T1 is 1 and T2 is 2. 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 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 Add 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 Add 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 Add 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.

4. On the Threshold Settings tab, click  **New** to configure the metrics for the threshold. For more information, see Adding New QoS Threshold Settings Using Add Threshold Settings Form.

Adding New QoS Threshold Settings Using Add Threshold Settings Form

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	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 the percentage is 80 and clear the incident when the percentage comes down to 60. Set the following values for the threshold: ▪ High Value: `80` ▪ High Value Rearm: `60` This value enables you to be aware when a network performance problem starts to improve.

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	Designate the minimum time within which the metric value must remain in the High range. 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. You define the high threshold value in the High Value field. 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..
High Duration Window	Designate the window of time within which the High Duration criteria must be met. To enable this setting, the value must be: ▪ greater than 0 (zero) ▪ the same as or greater than the High 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. 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.

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

3. Continue creating the threshold in the Add QoS Threshold Configuration form.

Saving the Threshold Using the Add Threshold Configuration Form

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.

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 Using the Edit Threshold Configuration Form

To edit an existing QoS threshold:

1. Launch the QoS Threshold Configuration form.
2. Select the threshold setting to modify, and click  **Edit**.

   The Edit QoS Threshold Configuration form opens.
3. 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 Add 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 Add 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 Add 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.

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.

Editing Existing QoS Threshold Settings Using Edit Threshold Settings Form

To configure the metrics for the threshold:

1. Make sure that you have specified the mandatory fields in the Edit Threshold Configuration.
2. Select the threshold settings, and Click  **Edit**
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.

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 the percentage is 90 and clear the incident when the percentage comes down to 60. Set the following values for the threshold: ▪ High Value: 90

Field Name	Description
	▪ High Value Rearm: 60 This value enables you to be aware when a network performance problem starts to improve.

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	Designate the minimum time within which the metric value must remain in the High range. 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. You define the high threshold value in the High Value field. 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..
High Duration Window	Designate the window of time within which the High Duration criteria must be met. To enable this setting, the value must be: ▪ greater than 0 (zero) ▪ the same as or greater than the High 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. 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.

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 NNM iSPI Performance for QA Threshold Incidents.

Saving the Threshold Using the Edit Threshold Configuration Form

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

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`

Deleting an Existing QoS Threshold Using the Threshold Configuration Form

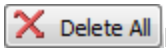
To delete an existing QoS threshold:

1. Launch the QoS Threshold Configuration form .
2. Select a threshold in the **Threshold Settings** panel and click  **Delete**.
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.

Deleting All Existing QoS Thresholds

To delete all the existing thresholds:

1. Launch the QoS Threshold Configuration form .
2. Click 

Delete All.
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 the existing thresholds.

Importing the QoS Threshold Configurations

To import threshold configurations from an XML file:

1. Launch the QoS Threshold Configuration form .
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/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:

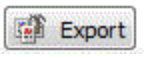
Linux: `$NnmDataDir/log/qa/qa.log`

Windows:`%NnmDataDir%\log\qa\qa.log`

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

Exporting the QoS Threshold Configurations

To export the existing threshold configurations to an XML file:

1. Launch the QoS Threshold Configuration form .
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.

QoS Threshold Configuration Metrics

You can configure threshold on the following metrics based on the selected device type:

CBQoS Metrics Metrics

Metric	Description
Pre Policy Bit Rate (kbps)	The bit rate of the traffic *per class* before applying the CBQoS policy, measured in kbps
Post Policy Bit Rate (kbps)	The bit rate of the traffic *per class* after applying the CBQoS policy, measured in kbps
Packet Drop (%)	Percentage of the packets dropped *per class*. It is calculated using the following formula: (Total number of dropped packets / total number of packets transmitted per class)*100
Exceeded Packets (%)	Percentage of the packets dropped *per class* due to exceeded policies It is calculated using the following formula: (Total number of packets dropped due to exceeded policies / total number of packets transmitted)*100
Violated Packets (%)	Percentage of the packets dropped *per class* due to violated policies It is calculated using the following formula: (Total number of packets dropped due to violated policies / total number of packets transmitted)*100
Discarded Packets (%)	Percentage of the packets dropped *per class* due to the queuing action It is calculated using the following formula: (Total number of packets dropped due to the queuing action / total number of packets transmitted)*100
Queue Utilization (%)	Utilization rate for the queue It is calculated using the following formula: (Queue depth/Maximum queue depth) * 100

Metric	Description
Queue Bandwidth Utilization (%)	Percentage of the bandwidth utilized *per class* Available only when the bandwidth reservation per class is measured as one of the following values: * As absolute value * As a percentage of the total bandwidth. It is calculated using the following formula: (PostPolicyBytes in kbps / Bandwidth configured in kbps) * 100
Dropped Shape Packets (%)	Percentage of packets dropped *per class* due to the shaping action 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
Delayed Shape Packets (%)	Percentage of packets delayed *per class* due to the shaping action. It is calculated using the following formula: (Total number of packets delayed due to the shaping action/total number of packets transmitted)*100
RED Packets Tail Drop (%)	Percentage of packets dropped *per class* due to greater number of packets in the queue than the maximum threshold It is calculated using the following formula: (Total number of packets dropped by the RED algorithm / total number of packets transmitted)*100
RED Packets Drop (%)	Percentage of packets dropped *per class* due to the buffer overflow It is calculated using the following formula: (Total number of packets dropped by the RED algorithm / total number of packets transmitted)*100

Metric	Description
Marked DSCP Packets (%)	Percentage of packets marked with IP DSCP bits *per class* The class sets a configured DSCP value for the incoming IP packets. It is calculated using the following formula: (Packets with the IP DSCP bit set / total number of packets transmitted) * 100
Marked IP Precedence Packets (%)	Percentage of packets marked with IP Precedence *per class* The class sets a configured Precedence value for the incoming IP packets. It is calculated using the following formula: (Packets with the IP precedence bit set / total number of packets transmitted) * 100
Marked FRDE Packets (%)	Percentage of packets marked with IP FRDE bits *per class* The class sets a configured FRDE value for the incoming IP packets. It is calculated using the following formula: (Packets with the IP FRDE bit set / total number of packets transmitted) * 100

NNM iSPI Performance for QA Threshold Configuration 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.

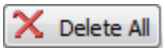
Adding New Threshold Settings to a QA Group

To add threshold settings to a QA Group:

1. Launch the QoS Threshold Configuration Form
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 the Threshold Settings Tab:

Icon	Description
 New	Adds a new QA Group threshold.
 Edit	Edits an existing QA Group threshold.
 Delete	Deletes an existing QA Group threshold.
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data.
 Delete All	Deletes all existing QA Group thresholds.

Creating New QoS Threshold Settings for a QA Group

To add a new threshold:

1. Specify all the mandatory fields in the Adding New Threshold Settings to a QA Group.
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 the percentage is 90 and clear the incident when the percentage comes down to 60. Set the following values for the threshold: ▪ High Value: `90` ▪ High Value Rearm: `60`

Field Name	Description
	This value enables you to be aware when a network performance problem starts to improve.

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	Designate the minimum time within which the metric value must remain in the High range. 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. You define the high threshold value in the High Value field. 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..
High Duration Window	Designate the window of time within which the High Duration criteria must be met. To enable this setting, the value must be: ▪ greater than 0 (zero) ▪ the same as or greater than the High 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. 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.

4. Select the following to generate an incident when the time-based threshold or count-based threshold value is violated:

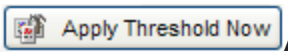
Field Name	Description
Generate Incident	Select this option if you want NNM iSPI Performance for QA to generate an incident for count-based or time-based threshold violations. By default this option is selected.

5. Use any one of the following options to complete the task:

Icons	Description
 Close	Closes the 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.

6. Continue creating the threshold in the Add QoS Threshold Configuration form.

7. After you configure the threshold settings, Click 

Apply Threshold Now in the QoS Threshold Configuration form, to apply the configured thresholds.

Editing the Existing Threshold Setting for a QA Group

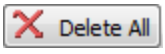
To edit an existing threshold setting for a QA Group:

1. Launch the QoS Threshold Configuration Form
2. Select the configured threshold settings to modify, and click  **Edit** in the QoS Threshold Configuration form.

   The Edit 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 Groups 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.

You can perform the following tasks in the Threshold Settings Tab:

Icon	Description
 New	Adds a new QA Groups Threshold Setting.
 Edit	Edits an existing QA Groups Threshold Setting.
 Delete	Deletes an existing QA Groups Threshold Setting.
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data.
 Delete All	Deletes all existing QA Groups Thresholds Setting.

Editing an Existing QoS Threshold Setting for a QA Group

To edit an existing threshold setting for a QA Group:

1. Specify all the mandatory fields in Editing the QA Group for QoS Threshold Settings.
2. Select the threshold setting to modify, and Click  **Edit** in the **Configured QoS Thresholds** panel.

   The Edit QoS 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. To see the metrics for each service type, click here.

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	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 the percentage is 90 and clear the incident when the percentage comes down to 60. Set the following values for the threshold:

Field Name	Description
	▪ High Value: 90 ▪ High Value Rearm: 60 This value enables you to be aware when a network performance problem starts to improve.

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:

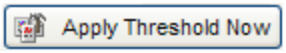
Field Name	Description
High Duration	Designate the minimum time within which the metric value must remain in the High range. For example if you specify this value to be 20 minutes for Packet Loss Percentage metric, NNM iSPI Performance for QA considers the threshold to be violated if the Packet Loss Percentage is high for 20 minutes. You define the high threshold value in the High Value field. 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..
High Duration Window	Designate the window of time within which the High Duration criteria must be met. To enable this setting, the value must be: ▪ greater than 0 (zero) ▪ the same as or greater than the High 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. 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.

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 an Existing Threshold Setting for a QA Group

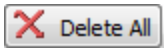
To delete an existing QoS threshold setting for a QA Group:

1. Launch the QoS Threshold Configuration Form.
2. Select one or more configured threshold settings in the **Configured QoS Thresholds** tab, and click  **Delete**.
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.

Deleting all Existing Thresholds for a QA Group

To delete all existing thresholds for a QA Group:

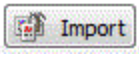
1. Launch the QoS Threshold Configuration Form.
2. Click 

Delete All.
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 QA Group Thresholds

To import threshold configurations from an XML file:

1. Launch the QoS Threshold Configuration Form .
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:

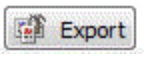
Linux: *$NnmDataDir/log/qa/qa.log*

Windows:*%NnmDataDir%\log\qa\qa.log*

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

Exporting the QA Group Thresholds

To export the existing QA Group threshold configurations:

1. Launch the QoS Threshold configuration Form .
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.

NNM iSPI Performance for QA QoS Discovery Filter Configuration

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

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.

Launching the QoS Discovery Filter Configuration Form

To launch the discovery filter configuration:

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

   You must have administrator privileges.

2. Select **Configuration** workspace.

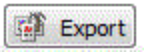
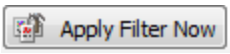
3. Select **Quality Assurance Configuration Console**

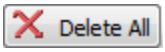
   The console opens.

4. In the **Configuration** workspace, select **QoS Discovery Filter**

   The QoS Discovery Filter Configuration form opens.

You can perform the following tasks using the QoS Discovery Filter Configuration form:

Icons Available in the QoS Discovery Filter Configuration Toolbar	Description
 Close	Closes the QoS Discovery Filter Configuration form without saving the current configuration
 Save	Saves the current configuration
 Save and Close	Saves the current configuration and closes the QoS Discovery Filter Configuration form
 Refresh	Retrieves the last saved QoS discovery filter configuration from the database
 Export	Exports the existing QoS discovery filter configuration
 Import	Imports QoS discovery filter configuration from an XML file
 Apply Filter Now	Applies the updated 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

Icons Available in the QoS Discovery Filter Configuration Toolbar	Description
	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 After you apply the discovery filter, run the discovery process to refresh the QoS Policies Inventory view based on the newly applied filters.
Icons Available in the Configured Filters Tab	**Description**
 New	Adds a new QoS discovery filter
 Edit	Edits an existing QoS discovery filter
 Delete	Deletes an existing QoS discovery filter
 Refresh	Retrieves the last saved QoS discovery filter configuration from the database and displays the data in the Configured Filters panel
 Delete All	Deletes all existing QoS discovery filters

Adding a New QoS Discovery Filter Using the QoS Discovery Filter Configuration Form

To add a new QoS discovery filter:

1. Launch the QoS Discovery Filter Configuration form.

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 **Add** to add the IP range to the list of IP ranges.
- You can select an IP range, and click Delete to remove it from the list of IP ranges.
- You can click Delete All **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 **Add** to add the node group to the list of node groups.
- You can select a node group, and click Delete to remove it from the list of node groups.
- You can click Delete All **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

Editing a QoS Discovery Filter Using the QoS Discovery Filter Configuration Form

To edit a discovery filter:

1. Launch the Discovery Filter Configuration form .
2. Select a filter in the 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 a New QoS Discovery Filter Using the QoS Discovery Filter Configuration Form.
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 Close	Saves the QoS discovery filter information and closes the Discovery Filter Configuration form

Deleting an Existing QoS Discovery Filter Using the QoS Discovery Filter Configuration Form

To delete an existing QoS discovery filter:

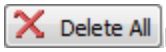
1. Launch the Discovery Filter Configuration form.
2. Select one or more filters in the **Configured Filters** panel in the Discovery Filter Configuration Form, and click  **Delete**.
3. Click  **Refresh** in the **Configured Filters** panel to view the changes.

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.

Deleting All Existing QoS Discovery Filters Using the QoS Discovery Filter Configuration Form

To delete all the existing QoS discovery filters:

1. Launch the QoS Discovery Filter Configuration form
2. Click 

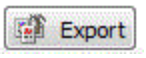
Delete All.
3. Click  **Refresh** in the **Configured Filters** panel to view the changes.

After you delete all QoS discovery filters, the filtered QoS elements are discovered in the next discovery cycle.

To refresh the QoS Policies Inventory view based on the deleted filters immediately, run the discovery process after you delete the discovery filters.

Exporting QoS Discovery Filter

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

1. Launch the QoS Discovery Filter Configuration form .
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: `$NnmDataDir/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 .
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.

NNM iSPI Performance for QA Probe Maintenance

The probes that are discovered can be enabled, disabled, or deleted using the Probe Maintenance form.

Launching the Probe Maintenance Form

Perform the following steps to launch the Probe Maintenance form:

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

   You must have administrator privileges.

2. Click **Quality Assurance** in the Workspaces panel. The list of probes that are discovered in your network appear in the content pane.

3. Select a probe and click **Actions** → **Quality Assurance** → **Probe Maintenance.** The Probe Maintenance form opens.

4. 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.

The Probe Maintenance form displays four tabs on the top of the user interface; Probe List, Enable Status, Disable Status, and Delete Status.

Probe Maintenance Form: Probe List Tab

You can use the **Probe List** tab to do the following tasks for the selected source and destination node:

- Enable QA probes
- Disable QA probes
- Delete QA probes

To view the probe list:

1. Launch the Probe Maintenance form.
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.

Field Name	Description
Service	The service type of the QA probe. The valid service types are: ▪ 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.

Probe Maintenance Form: Enable Status Tab

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.
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.

Probe Maintenance Form: Disable Status Tab

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.
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.

Probe Maintenance Form: Delete Status Tab

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.
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.

NNM iSPI Performance for QA File-Based Node Discovery Configuration

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.

NNM iSPI Performance for QA Discovery Filter Configuration

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.

NNM iSPI Performance for QA Site Configuration

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`

NNM iSPI Performance for QA Threshold Configuration

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.
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.

NNM iSPI Performance for QA Global Network Management Configuration

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:`%NnmDataDir%\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.

Use Case for NNM iSPI Performance for QA 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`.
4. Click  **New** in the Threshold Settings panel.

   The Add Threshold Settings form opens.
5. 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

6. Click  **Save and Close**

   The Add Threshold Settings form closes.

7. Click  **Save** in the Site Wide Threshold Configuration form.

8. Click  **Refresh** in the Threshold Settings panel to view the threshold for the Two Way Jitter.

Process Termination

1. Close the Add Threshold Configuration form by selecting any of the following options:
   - Click  **Save and Close**
   - Click  **Save** and then click  **Close**.
2. 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

NNM iSPI Performance for QA 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.

NNM iSPI Performance for QA 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.

QA Threshold Configuration Metrics

You can configure threshold on the following metrics based on the selected service type.

QA Threshold Metrics

Probe Service Types	Vendors
	Cisco
ICMP Echo	• Round Trip Time (ms) • Round Trip Time (microseconds)
UDP Echo	• Round Trip Time (ms) • Round Trip Time (microseconds)
UDP	• Round Trip Time (ms) • Round Trip Time (microseconds) • Positive Jitter SD • Positive Jitter DS • Negative Jitter SD • Negative Jitter DS • Packet Loss SD (%) • Packet Loss SD (%) • Two way Jitter • Two way Packet Loss (%)
TCP Connect	• Round Trip Time (ms) • Round Trip Time (microseconds)
VoIP	• Round Trip Time (ms) • Round Trip Time (microseconds)

	• Positive Jitter SD • Positive Jitter DS • Negative Jitter SD • Negative Jitter DS • Packet Loss SD (%) • Packet Loss SD (%) • Two way Jitter • Two way Packet Loss (%) • Mean Opinion Score (MOS)
Oracle	Not supported
HTTP	• Round Trip Time (ms) • Round Trip Time (microseconds)
HTTPS	Not supported
DNS	• Round Trip Time (ms) • Round Trip Time (microseconds)
DHCP	• Round Trip Time (ms) • Round Trip Time (microseconds)

We appreciate your feedback!

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Online Help (Network Node Manager iSPI Performance for Quality Assurance 10.00)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to docfeedback@hp.com.