HP Network Node Manager i Software Smart Plug-in Performance for Quality Assurance

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

Software Version: 9.00

Online Help

Document Release Date: April 2010

Software Release Date: April 2010

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

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

Copyright Notices

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

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

This product includes Commons Discovery software developed by the Apache Software Foundation (http://www.apache.org/). Copyright © 2002-2008 The Apache Software Foundation. All Rights Reserved.

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

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

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

Trademark Notices

DOM4J® is a registered trademark of MetaStuff, Ltd.

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

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

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

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

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

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

Table of Contents

HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA) Help for Administrators

NNM iSPI Performance for QA enables you to:

- Discover the QA probes configured in the network managed by HP Network Node Manager i-Suite Software (NNMi).
- Analyze the outcome of each QA probe for past one day, one week, and one month.

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

- Not Managed
- Out of Service

NNM iSPI Performance for QA measures the network performance using the following metrics:

- **Round Trip Time (RTT)**[1]
- **Jitter**[2]
- Packet loss (Can be from source to destination, from destination to source, or two way.)

For information on metrics, see NNM iSPI Performance for QA Metrics in the *HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA) Reports Online Help*.

NNM iSPI Performance for QA loads the network performance information in NNMi using the following MIBs:

- CISCO-RTTMON-MIB
- DISMAN-PING-MIB

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

- **IP SLA**[3]
- DISMAN Ping using RFC 4560

To enable basic monitoring of your network traffic performance, log on to the NNMi console with administrator credentials. You can then view the following:

- NNM iSPI Performance for QA workspace: Access the inventory view to monitor the status and necessary details for the pre-configured QA probes in every device in your network.
- NNM iSPI Performance for QA configuration: In the Configuration tab, you can find Quality Assurance Site Configuration and Quality Assurance Threshold Configuration features to configure the sites and threshold settings for the QA probes.

[1] The time required for a signal pulse or packet to travel from a specific source to a specific destination and back again.

[2] Jitter is a measure of the variability over time of the latency across a network. A very low amount of jitter is important for real-time applications using voice and video. Jitter can be positive, negative, from source to destination, and from destination to source.

[3] Cisco IOS IP SLAs is a feature included in the Cisco IOS Software that can allow administrators the ability to Analyze IP Service Levels for IP applications and services. IP SLA's uses active traffic-monitoring technology to monitor continuous traffic on the network. Using IP SLAs, routers and switches perform periodic measurements. The exact number and type of available measurements depends on the IOS version.

For more information on accessing the Quality Assurance workspace, see Accessing the Quality Assurance Workspace.

For more information on accessing the QA Probes view, see Accessing the QA Probes View.

Discovering QA Probes Using nmsqadisco.ovpl Command

HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA) discovers the QA probes configured in the network managed by HP Network Node Manager i-Suite Software (NNMi) during each NNMi discovery.

Use the following command to discover the QA probes configured on the managed NNMi nodes independently:

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

Parameters

- -u <username>: Supply the NNMi administrator username required to execute the command. This is a required parameter.
- -p <password>: Supply the NNMi administrator password required to execute the command. This is a required parameter.
- -node <nodename>: Supply the node name to run the discovery process on selected nodes.
- -all: Use this parameter to run the discovery process on all the managed nodes.

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

HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA)Discovery Filter Configuration

You might have numerous tests configured in your entire network. Not all of these QA probes are always useful to you to analyze, monitor, or measure network performance. HP Network Node Manager i-Suite Software (NNMi) updates the QA probe information during each discovery process and monitors the discovered QA probes regularly.

This feature can sometimes hamper your network performances analysis, as some of the QA probes (like the interface health reporting QA probes) produce a lot of output that may not be required for network performance monitoring.

NNM iSPI Performance for QA enables you to filter the discovery process based on the owners associated to the QA probes.

Using this feature, you can exclude the QA probes you do not require based on the QA probe owners. This feature immediately removes the QA probes from the database. The poller stops polling these QA probes subsequently. Consequently these QA probes get excluded from the QA Probes view.

Launching the Discovery Filter Configuration

To launch the discovery filter configuration:

1. Log on to NNMi console using your username and password.

   You must have administrator privileges.

2. Click **Configuration**. The Configuration tab expands.
3. Select **Quality Assurance Discovery Filter Configuration**.

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

Tasks Available in the Discovery Filter Configuration Toolbar	Description
Close	Closes the Discovery Filter Configuration form without saving the current configuration.
Save	Saves the current configuration.
Save and Close 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 Apply Filter Now	Applies the filters on the NNMi discovery process.
Export Export	Exports the existing discovery filter configuration
Import Import	Imports discovery filter configuration from an XML file

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 QA Probe Filtering** to activate the discovery filters.
3. Enter the QA probe owner name or a pattern suggesting the owner name in the Exclude Test Owner Name Patterns box.

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

4. Click Add **Add**. The new QA probe owner name is added to the list in the Excluded Probe Owner Names & Patterns box.

   Select a QA probe owner name and click Delete **Remove** to remove it from the Excluded Probe Owner Names & Patterns box.

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

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

Option	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 **Save and Close**	Save the discovery filter information and closes the Discovery Filter Configuration form
Apply Filter Now Apply Filter Now	Applies the discovery filters immidiately and excludes the QA probes owned by the specified owner names from the QA Probes view.

6. Click **Refresh** in the Discovery Filter Configuration form to view the changes.

Exporting a Discovery Filter Using Discovery Filter Configuration Form

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

1. Launch the Discovery Filter Configuration form.
2. Click Export **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`.
4. Click **OK** in the user prompt dialog.

If the discovery filter export fails, check the following log files:

UNIX: *./var/opt/OV/log/qa/qaspi0.log*

By default, the %QASPI_Install_Dir% is <*drive:*> */opt/OV*

Windows: *%QASPI_Install_Dir%\log\qa\qaspi0.log*

By default, the %QASPI_Install_Dir% is <*drive*>*:\Program Files(x86)\HP\HP BTO Software*

Importing Discovery Filters Using Discovery Filter Configuration Form

To import discovery filter configurations from an XML file and display them in the Discovery Filter Configuration form:

1. Launch the Discovery Filter Configuration form.
2. Click Import **Import**.
3. In the user prompt dialog, 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** in the user prompt dialog.

   If a site 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.

If the discovery filter import fails, check the following log files:

UNIX: *./var/opt/OV/log/qa/qaspi0.log*

By default, the %QASPI_Install_Dir% is *<drive:> /opt/OV*

Windows: *%QASPI_Install_Dir%\log\qa\qaspi0.log*

By default, the %QASPI_Install_Dir% is *<drive>:\Program Files(x86)\HP\HP BTO Software*

HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA)Site Configuration

NNM iSPI Performance for QA enables you to analyze the network performances of different **network elements**[1]. Logically grouping the networking devices into **sites**[2] enables you to get an overview of your network performance.

Example

An enterprise network with branch offices is connected to the head office via WAN links. Measuring the network performances for different network elements can prove time-consuming and cumbersome. On the other hand, measuring the network performances across all the offices and comparing the network performance of the head office and the branch offices can be useful in giving you an overview of traffic performance throughout the network.

You can configure Quality Assurance (QA) probes between individual nodes or node groups and assign them to the sites. Also, you can assign the thresholds for the metrics to the sites and analyze the site performance based on these thresholds.

Launching the Site Configuration form

Perform the following steps to launch the site configuration form:

1. Log on to HP Network Node Manager i-Suite Software (NNMi) console using your username and password.

   You must have administrator privileges.

[1] Examples of network elements are; source node, destination node, QA probe name, QA probe type, source site, destination site, class of service, QA probe UUID, node UUID, etc.

[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 gegraphic 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. Click **Configuration**. The Configuration tab expands.
3. Select **Quality Assurance Site Configuration**.

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

Tasks Available in the Site Configuration Toolbar	Description
Close	Closes the Site Configuration form without saving the current configuration.
Save	Saves the current configuration.
Save and Close Save and Close	Saves the current configuration and closes the Site Configuration form.
Refresh	Retrieves the last saved site configuration from the database and displays the data in the Configured Sites panel of the Site Configuration form.
Recompute Probes Associations Recompute QA Probe Configurations	Re-assigns the QA probes to the sites
Export Export	Exports the existing sites
Import Import	Imports sites from an XML file
Tasks Available in the Global Settings Panel	**Description**
Enable Site Configuration	Enables you to configure sites. If this option is not selected, you will not be able to use the Configured Sites panel.
Tasks Available in the Configured Sites Panel	**Description**
New	Adds a new 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 Delete All	Deletes all the existing sites

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.

      Site names cannot contain **'** (single quotation marks).

      When you rename a site, it is identified by the new name.

   b. **Ordering**

      A QA probe can be associated to only one 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.

      If a QA probe matches multiple sites, the site with the lower ordering gains priority to run the QA probe.

      ### Example 1

      The discovered QA probe name "`UDP QA probe from Site A over WAN link to SiteB`" is associated to both SiteA and SiteB. The ordering number for SiteA is `1`, and the ordering number for SiteB is `2`. SiteA is given priority to run `UDP QA probe from Site A over WAN link to SiteB`.

      If a QA probe is associated to multiple sites and the ordering is the same for both sites, the weights of the **site rules**[2] are used to resolve the conflict. The weights are inherent to the site rules.

[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 the lowest priority among these foure 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 the rules.

[2] 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 the lowest priority among these foure 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 the rules.

Example 2

The discovered QA probe name "`UDP QA probe from Site A over WAN link to SiteB`" is associated to 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 to 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, while you add them to a site.

The node group must be discovered by HP Network Node Manager i-Suite Software (NNMi) and present in the NNMi database.

d. **IP Address Range**

Type the IP address or IP address range and click Add **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 **Delete** to remove it from the IP Address Range box.

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

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**[1].

e. **Probe Name Patterns**

The Probe Name Patterns box lists the QA probes associated to the node group.

By default NNM iSPI Performance for QA populates the Probe Name Patterns box with the QA probe names associated to 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 **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 as described below, while specifying a QA probe pattern:

- If the QA probe name pattern includes both source and destination information, use a delimiter to differentiate between the source and destination information.

  The QA probe pattern should 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 the source information.
- The string on the right hand side of the delimiter is considered 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`" should contain the string "`SiteA`".
- The destination information on the right hand side of the delimiter "`over`" should contain the string "`SiteB`" followed by 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.

[1] IPv6 addresses are generally written in the form, hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh. In this full notation, pairs of IPv6 bytes are separated by a COLON and each byte in turns is represented as a pair of hexadecimal numbers. For example, E3D7:0000:0000:0000:51F4:9BC8:C0A8:6420. Shorthand notation in IPv6 removes these bytes with a zero values from the text representation, though the bytes still remain present in the actual network address). For example, E3D7::51F4:9BC8:C0A8:6420.

Example 2

QA Probe Name Pattern: remote site???|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`" should contain the string "`remote site`", followed by three characters.
- The destination information on the right hand side of the delimiter "to" should contain the string "`central`" followed by any number of characters.

If you have QA probes named "`SiteA remote office123 to central office In SiteB`", "`SiteC remote office254 to central office In SiteB`", and "`SiteD remote office356 to central office In SiteB`**"**

Select an QA probe name and click Delete **Remove** 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.

f. **VRF Wildcards**

If your site is associated to a Virtual Private Network (VPN), NNM iSPI Performance for QA populates the VRF Wildcards box with the available **VRF**[1] ranges.

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

Option	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 **Save and Close**	Saves the site information and closes the Add Site Configuration form

[1] Virtual Routing and Forwarding (VRFs) tables include the routing information that defines the Virtual Private Network (VPN) attached to a Provider Edge (PE) router. Each VRF is on a PE router. All PE routers containing VRFs relevant to the named VPN are grouped in one VPN. A VRF can only belong to a single VPN and is grouped on the basis of the Route Targets.

Option	Description
Clear	Clears the site information you have entered in the 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 panel and click **Edit**.

   The Edit Site Configuration form opens.
3. Update the following values as required:
   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.

   Site names cannot contain **'** (single quotation marks).

   When you rename a site, it is identified by the new name.

   Ordering

   A QA probe can be associated to only one 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.

   If a QA probe matches multiple sites, the site with the lower ordering gains priority to run the QA probe.

   ### Example 1

   The discovered QA probe name "`UDP QA probe from Site A over WAN link to SiteB`" is associated to both SiteA and SiteB. The ordering number for SiteA is `1`, and the ordering number for SiteB is `2`. SiteA is given priority to run `UDP QA probe from Site A over WAN link to SiteB`.

   If a QA probe is associated to 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.

[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 the lowest priority among these foure 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 the rules.

Example 2

The discovered QA probe name "`UDP QA probe from Site A over WAN link to SiteB`" is associated to 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 to 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 HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA) assigns a site the lowest ordering value.

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, while you add them to a site.

The node group must be discovered by HP Network Node Manager i-Suite Software (NNMi) and present in the NNMi database.

IP Address Range

Type the IP address or IP address range and click Add **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 **Delete** to remove it from the IP Address Range box.

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

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**[1].

Probe Name Pattern

The Probe Name Patterns box lists the QA probes associated to the node group.

By default NNM iSPI Performance for QA populates the Probe Name Patterns box with the QA probe names associated to 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 **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 as described below, while specifying a QA probe pattern:

- If the QA probe name pattern includes both source and destination information, use a delimiter to differentiate between the source and destination information.

  The QA probe pattern should 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 the source information.
- The string on the right hand side of the delimiter is considered 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`" should contain the string "`SiteA`".
- The destination information on the right hand side of the delimiter "`over`" should contain the string "`SiteB`" followed by 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.

[1] IPv6 addresses are generally written in the form, hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh. In this full notation, pairs of IPv6 bytes are separated by a COLON and each byte in turns is represented as a pair of hexadecimal numbers. For example, E3D7:0000:0000:0000:51F4:9BC8:C0A8:6420. Shorthand notation in IPv6 removes these bytes with a zero values from the text representation, though the bytes still remain present in the actual network address). For example, E3D7::51F4:9BC8:C0A8:6420.

Example 2

QA Probe Name Pattern: remote site???|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`" should contain the string "`remote site`", followed by three characters.
- The destination information on the right hand side of the delimiter "to" should contain the string "`central`" followed by any number of characters.

If you have QA probes named "`SiteA remote office123 to central office In SiteB`", "`SiteC remote office254 to central office In SiteB`", and "`SiteD remote office356 to central office In SiteB`**"**

Select an QA probe name and click Delete **Remove** 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.

VRF Wildcards

If your site is associated to a Virtual Private Network (VPN), NNM iSPI Performance for QA populates the VRF Wildcards box with the available **VRF**[1] ranges.

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

Option	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 **Save and Close**	Saves the site information and closes the Edit Site Configuration form

[1] Virtual Routing and Forwarding (VRFs) tables include the routing information that defines the Virtual Private Network (VPN) attached to a Provider Edge (PE) router. Each VRF is on a PE router. All PE routers containing VRFs relevant to the named VPN are grouped in one VPN. A VRF can only belong to a single VPN and is grouped on the basis of the Route Targets.

Option	Description
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.

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 **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.

Exporting a Site Using Site Configuration Form

To export the existing site configurations to an XML file:

1. Launch the Site Configuration form.
2. Click Export **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`.
4. Click **OK** in the user prompt dialog.

You can also export the existing site configuration using the following command line utility:

UNIX: *. %QASPI_Install_Dir%/bin/nmsqasiteconfigutil.ovpl –export [filename]*

Windows: *%QASPI_Install_Dir%\bin\nmsqasiteconfigutil.ovpl –export [filename]*

If the site export fails, check the following log files:

UNIX: *./var/opt/OV/log/qa/qaspi0.log*

By default, the %QASPI_Install_Dir% is <*drive:*> */opt/OV*

Windows: *%QASPI_Install_Dir%\log\qa\qaspi0.log*

By default, the %QASPI_Install_Dir% is *<drive>:\Program Files(x86)\HP\HP BTO Software*

Importing Sites Using Site Configuration Form

To import site configurations from an XML file and display them in the Configured Sites panel of the Site Configuration form:

1. Launch the Site Configuration form.
2. Click Import **Import**.
3. 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`.
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:

UNIX:*.%QASPI_Install_Dir%/bin/nmsqasiteconfigutil.ovpl –import [filename]*

Windows: *%QASPI_Install_Dir%\bin\nmsqasiteconfigutil.ovpl –import [filename]*

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

UNIX: *./var/opt/OV/log/qa/qaspi0.log*

By default, the %QASPI_Install_Dir% is *<drive:> /opt/OV*

Windows: *%QASPI_Install_Dir%\log\qa\qaspi0.log*

By default, the %QASPI_Install_Dir% is *<drive>:\Program Files(x86)\HP\HP BTO Software*

Re-Computing Site Configurations

HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA) associates the QA probes with the respective sites during the configuration poll.

User Scenario

The head office of an organization is connected to it's 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`

Ordering: `1`

Node Group: `Routers`

IP Address Range: `17.1-100.*.*`

Probe Name Patterns: `*SiteA|to|Central`

VRF Wildcards: None

Later, the following QA probe name patterns need to be added to SiteA:

- SiteA???|to|*Central
- SiteA*|over|Central*

Also, the following VRF groups need to be added:

- 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 to SiteA in the next configuration poll.

Use the Recompute QA Probe Associations utility to associate the QA probes to the new or updated sites at once.

Use any of the following options 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:
  - **UNIX:** *.%QASPI_Install_Dir% /bin/nmsqasiteconfigutil.ovpl –recompute*

    By default, the %QASPI_Install_Dir% is *<drive:> /opt/OV*
  - **Windows:** *%QASPI_Install_Dir%\bin\nmsqasiteconfigutil.ovpl –recompute*

    By default, the %QASPI_Install_Dir% is *<drive>:\Program Files(x86)\HP\HP BTO Software*

HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA)Threshold Configuration

NNM iSPI Performance for QA thresholds enables you track the health and performances of the **network elements**[1] and monitor the traffic flow. You can configure the thresholds to generate exceptions. The NNM iSPI Performance for QA displays the exception counts.

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

A threshold must have a source site, but might 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 any of the following Quality Assurance metrics derived from the QA probes configured for an existing site:

- **Round Trip Time (RTT)**[2]
- **Jitter**[3]

[1] Examples of network elements are; source node, destination node, QA probe name, QA probe type, source site, destination site, class of service, QA probe UUID, node UUID, etc.

[2] The time required for a signal pulse or packet to travel from a specific source to a specific destination and back again.

[3] Jitter is a measure of the variability over time of the latency across a network. A very low amount of jitter is important for real-time applications using voice and video. Jitter can be positive, negative, from source to destination, and from destination to source.

- Packet Loss (Can be from source to destination, and from destination to source.)
- **Mean Opinion Scores(MOS)**[1]

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.

A QA probe status becomes critical only if the operator status times out.

Launching the Threshold Configuration form

To launch the threshold configuration form:

1. Log on to HP Network Node Manager i-Suite Software (NNMi) console using your username and password.

   You must have administrator privileges.

2. Click **Configuration**. The Configuration tab expands.
3. Select **Quality Assurance Threshold Configuration**.

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

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

Tasks 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 thresholds
Import	Imports thresholds from an XML file
Tasks Available in the Global Settings Panel	**Description**
Enable Site wide threshold configuration	Enables you to configure thresholds. If this option is not selected, you will not be able to use the Site Wide Threshold Settings panel and no thresholds will be applied in the poller.

[1] A measurement of the subjective quality of human speech, represented as a rating index. MOS is derived by taking the average of numerical scores given by juries to rate quality and using it as a quantitative indicator of system performance.

Tasks Available in the Threshold Configuration Toolbar	Description

Tasks Available in the Configured Sites Panel	Description
New	Adds a new threshold
Edit	Edits an existing threshold
Delete	Deletes an existing threshold
Refresh	Retrieves the last saved threshold configuration from the database and displays the data in the Site Wide Threshold Settings panel.
Delete All Delete All	Deletes all the existing thresholds

Adding New Threshold Settings Using the Threshold Configuration Form

To add a new threshold:

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

   The Add Threshold Configuration form opens.
3. The new threshold is assigned to the QA probes configured to an existing site.

   Specify the following information in the Threshold Configuration panel:

Field Name	Description
Source Site	Select the name of the site from which the QA probes will be ini-

Field Name	Description
	tiated.
Destination Site	Select the destination for the QA probes. Specifying a destination site is optional in threshold configuration.
Service	The type of the discovered QA probe NNM iSPI Performance for QA recognizes the following QA probe types: ■ **UDP Echo**[1] ■ **ICMP Echo**[2] ■ **UDP**[3] ■ **TCP Connect**[4] ■ **VoIP**[5]

4. Click **New** in the Threshold Settings panel.

   The Add Threshold Settings form opens.

5. Specify the following values to configure the new threshold:

[1] A UDP Echo is a server program that gives you an echo of a text string that you send using a UDP client.

[2] ICMP Echo is a method used to test whether a particular host is reachable across an IP network; it is also used to self test the network interface card of the computer, or as a latency test. It measures the round-trip time and records any packet loss, response packets received, the minimum, mean, maximum and the standard deviation of the round trip time.

[3] The User Datagram Protocol (UDP) is one of the core members of the Internet Protocol Suite. UDP service type in QA SPI uses the UDP protocol and provides jitter measurements. With UDP protocol, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths.

[4] TCP Connect scans a normal TCP connection to determine if a port is available. This scan method uses the same TCP handshake connection that every other TCP-based application uses on the network.

[5] Voice over Internet Protocol (VoIP) is a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks. VoIP converts an analog voice signal to digital format and compresses the signal into Internet protocol (IP) packets for transmission over the Internet.

Field Name	Description
Metric	Select the name of the metric for which you are creating the threshold. For **Round Trip Time (RTT)**[1] and **Jitter**[2] select the threshold precision. You can select any of the following precisions: - Microseconds - Milliseconds The Packet Loss metric is measured in percentage.
High Value	Enter the threshold value.
High Value Rearm	Enter the high rearm value for the threshold. NNM iSPI Performance for QA generates an incident for a threshold violation, based on your selection. The rearm value specifies the threshold value when such an incident should be cleared. In other words the rearm value specifies the acceptable value for a metric. The high value rearm must always be lower than the high value. **Example** For the **Round Trip Time (RTT)**[3] 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.
Low Value	Enter the threshold value.
Low Value Rearm	Enter the low rearm value for the threshold. NNM iSPI Performance for QA generates an incident for a thresh-

[1] The time required for a signal pulse or packet to travel from a specific source to a specific destination and back again.

[2] Jitter is a measure of the variability over time of the latency across a network. A very low amount of jitter is important for real-time applications using voice and video. Jitter can be positive, negative, from source to destination, and from destination to source.

[3] The time required for a signal pulse or packet to travel from a specific source to a specific destination and back again.

Field Name	Description
	old violation, based on your selection. The rearm value specifies the threshold value when such an incident should be cleared. In other words the rearm value specifies the acceptable value for a metric. The low value rearm must be greater than the low value. **Example** For the **Mean Opinion Scores(MOS)**[1] 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.
Trigger Count	Specify after how many threshold violations NNM iSPI Performance for QA should set the QA probe status to ▼ **Major**.
Generate Incident	Select this option if you want NNM iSPI Performance for QA to generate incidents upon threshold violations. By default this option is selected.

Use any of the following options to complete the task:

Option	Description
Close	Closes the Add Threshold Configuration form without saving the threshold information you have entered.
Save and Close **Save and Close**	Saves the threshold information and closes the Threshold Configuration form
Clear	Clears the threshold information you have entered in the form

6. Click **Refresh** in the Threshold Settings panel to view the changes.
7. Click **Save** or Save and Close **Save and Close** in the Site Wide Threshold Configuration form.

[1] A measurement of the subjective quality of human speech, represented as a rating index. MOS is derived by taking the average of numerical scores given by juries to rate quality and using it as a quantitative indicator of system performance.

Caution: The new threshold will not be saved unless you click **Save** or Save and Close **Save and Close** in the Site Wide Threshold Configuration form.

NNM iSPI Performance for QA applies the following rules while creating thresholds:

- You can create thresholds only for the existing sites.
- You must select a source site 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.

Edit an Existing Threshold Using the Threshold Configuration Form

To edit an existing threshold:

1. Launch the Threshold Configuration form.
2. Click **Edit** in the Site Wide Threshold Settings panel.

   The Edit Threshold Configuration form opens.
3. This form displays the site information for the threshold.

   You can modify the following information in the Site Configuration Details panel:

Field Name	Description
Source Site	Select the name of the site from which the QA probes will be initiated.
Destination Site	Select the destination for the QA probes. Specifying a destination site is optional in threshold configuration.
Service	The type of the discovered QA probe NNM iSPI Performance for QA recognizes the following QA probe types:

Field Name	Description
	■ **UDP Echo**[1] ■ **ICMP Echo**[2] ■ **UDP**[3] ■ **TCP Connect**[4] ■ **VoIP**[5]

4. Click ✎ **Edit** in the Site Wide Threshold Settings panel.

   The Threshold Configuration form opens.

5. You can modify the following information:

Field Name	Description
Metric	Select the name of the metric for which you are creating the threshold. For **Round Trip Time (RTT)**[6] and **Jitter**[7] select the threshold precision. You can select any of the following precisions: ■ Microseconds ■ Milliseconds The Packet Loss metric is measured in percentage.

[1] A UDP Echo is a server program that gives you an echo of a text string that you send using a UDP client.

[2] ICMP Echo is a method used to test whether a particular host is reachable across an IP network; it is also used to self test the network interface card of the computer, or as a latency test. It measures the round-trip time and records any packet loss, response packets received, the minimum, mean, maximum and the standard deviation of the round trip time.

[3] The User Datagram Protocol (UDP) is one of the core members of the Internet Protocol Suite. UDP service type in QA SPI uses the UDP protocol and provides jitter measurements. With UDP protocol, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths.

[4] TCP Connect scans a normal TCP connection to determine if a port is available. This scan method uses the same TCP handshake connection that every other TCP-based application uses on the network.

[5] Voice over Internet Protocol (VoIP) is a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks. VoIP converts an analog voice signal to digital format and compresses the signal into Internet protocol (IP) packets for transmission over the Internet.

[6] The time required for a signal pulse or packet to travel from a specific source to a specific destination and back again.

[7] Jitter is a measure of the variability over time of the latency across a network. A very low amount of jitter is important for real-time applications using voice and video. Jitter can be positive, negative, from source to destination, and from destination to source.

Field Name	Description
High Value	Enter the threshold value.
High Value Rearm	Enter the high rearm value for the threshold. NNM iSPI Performance for QA generates an incident for a threshold violation, based on your selection. The rearm value specifies the threshold value when such an incident should be cleared. In other words the rearm value specifies the acceptable value for a metric. The high value rearm must always be lower than the high value. **Example** For the **Round Trip Time (RTT)**[1] 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.
Low Value	Enter the threshold value.
Low Value Rearm	Enter the low rearm value for the threshold. NNM iSPI Performance for QA generates an incident for a threshold violation, based on your selection. The rearm value specifies the threshold value when such an incident should be cleared. In other words the rearm value specifies the acceptable value for a metric. The low value rearm must be greater than the low value. **Example** For the **Mean Opinion Scores(MOS)**[2] 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`

[1] The time required for a signal pulse or packet to travel from a specific source to a specific destination and back again.

[2] A measurement of the subjective quality of human speech, represented as a rating index. MOS is derived by taking the average of numerical scores given by juries to rate quality and using it as a quantitative indicator of system performance.

Field Name	Description
	This value enables you to be aware when a network performance problem starts to improve.
Trigger Count	Specify after how many threshold violations NNM iSPI Performance for QA should set the QA probe status to **Major**.
Generate Incident	Select this option if you want NNM iSPI Performance for QA to generate incidents upon threshold violations. By default this option is selected.

Use any of the following options to complete the task:

Option	Description
Close	Closes the Add Threshold Configuration form without saving the threshold information you have entered.
Save and Close **Save and Close**	Saves the threshold information and closes the Threshold Configuration form
Clear	Clears the threshold information you have entered in the form

6. Click **Refresh** in the Threshold Settings panel to view the changes.
7. Click Save and Close **Save and Close**.

   The Threshold Configurations form closes.
8. Click **Save** or Save and Close **Save and Close** in the Site Wide Threshold Configuration form.

Caution: The changes you have made in the threshold will not be saved unless you click **Save** or Save and Close **Save and Close** in the Site Wide Threshold Configuration form.

NNM iSPI Performance for QA applies the following rules while updating thresholds:

- You can define thresholds only for the existing sites.
- You must select a source site for the threshold.
- You could select the destination site for the 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.
- Any modification in the threshold directly updates the state poller.

Delete an Existing Threshold Using the Threshold Configuration UI

To delete an existing threshold:

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

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

The thresholds are deleted from the configuration poller immediately.

Delete All Existing Thresholds Using the Threshold Configuration UI

To delete all the existing thresholds:

1. Launch the Threshold Configuration form.
2. Click **Delete All**.

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

The thresholds are deleted from the configuration poller immediately.

Exporting a Threshold Using Threshold Configuration Form

To export the existing threshold configurations to an XML file:

1. Launch the Threshold Configuration form.
2. Click **Export**.
3. Enter the file name where you want to export the existing threshold configuration in the user prompt dialog.

   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.

You can also export the existing threshold configuration using the following command line utility:

UNIX: *. %QASPI_Install_Dir%/bin/nmsqathresoldconfigutil.ovpl –export [filename]*

Windows: *%QASPI_Install_Dir%\bin\nmsqathresoldconfigutil.ovpl–export [filename]*

The threshold export utility does not export a threshold unless the threshold is associated to at least one site.

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

UNIX: *./var/opt/OV/log/qa/qaspi0.log*

By default, the %QASPI_Install_Dir% is *<drive:> /opt/OV*

Windows: *%QASPI_Install_Dir%\log\qa\qaspi0.log*

By default, the %QASPI_Install_Dir% is *<drive>:\Program Files(x86)\HP\HP BTO Software*

Importing Thresholds Using Threshold Configuration Form

To import threshold configurations from an XML file and display them in the in the Threshold Settings panel of the Threshold Configuration form:

1. Launch the 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:

UNIX: *. %QASPI_Install_Dir%/bin/nmsqathresoldconfigutil.ovpl –import [filename]*

Windows: *%QASPI_Install_Dir%\bin\nmsqathresoldconfigutil.ovpl–import [filename]*

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

UNIX: *./var/opt/OV/log/qa/qaspi0.log*

By default, the %QASPI_Install_Dir% is *<drive:> /opt/OV*

Windows: *%QASPI_Install_Dir%\log\qa\qaspi0.log*

By default, the %QASPI_Install_Dir% is *<drive>:\Program Files(x86)\HP\HP BTO Software*

HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA) Discovery Filter Configuration

QA probe filering is not enabled. Please enable it.

Occurs if you have not enable the test filtering option in the Discovery Filter Configuration form.

Reason and Resolution

Select the Enable Probes Filtering by Owner Name 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:

UNIX: *./var/opt/OV/log/qa/qaspi0.log*

Windows: *%QASPI_Install_Dir%\log\qa\qaspi0.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:

UNIX: *./var/opt/OV/log/qa/qaspi0.log*

Windows: *%QASPI_Install_Dir%\log\qa\qaspi0.log*

Failed to start filtering the QA probes. Please check the log files.

Occurs when the NNM iSPI Performance for QA fails to start filtering the QA probes based on the specified owner's names.

Reason and Resolution

Check any of the following log files:

UNIX: *./var/opt/OV/log/qa/qaspi0.log*

Windows: *%QASPI_Install_Dir%\log\qa\qaspi0.log*

Failed to delete the QA probe owner's name. Please check the log files.

Occurs when the NNM iSPI Performance for QA fails to delete the selected discovery filter configuration from the database.

Reason and Resolution

Check any of the following log files:

UNIX: *./var/opt/OV/log/qa/qaspi0.log*

Windows: *%QASPI_Install_Dir%\log\qa\qaspi0.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 QUOTE) as a QA probe owner name. NNM iSPI Performance for QA does not accept this character in a QA probe owner name.

HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA) Site Configuration

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 ne unique.
- If the IP address range is not valid.
- If the node group you specified does not exist in the HP Network Node Manager i-Suite Software (NNMi) database.

Resolution

Check any of the following log files:

UNIX: *./var/opt/OV/log/qa/qaspi0.log*

Windows: *%QASPI_Install_Dir%\log\qa\qaspi0.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.

Ordering 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.

Site Name cannot be blank

Occurs if you try to create a site without entering a value in the Site Name field in the Add Site Configuration form.

Reason and Resolution

NNM iSPI Performance for QA recognizes a site by its name.

You cannot create a site without a name.

Failed to start the recomputation of QA probes associations. Please check the log files.

Occurs when the NNM iSPI Performance for QA fails to start recomputation of QA probe associations.

Reason and Resolution

Check any of the following log files:

UNIX: *./var/opt/OV/log/qa/qaspi0.log*

Windows: *%QASPI_Install_Dir%\log\qa\qaspi0.log*

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:

UNIX: *./var/opt/OV/log/qa/qaspi0.log*

Windows: *%QASPI_Install_Dir%\log\qa\qaspi0.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:

UNIX: *./var/opt/OV/log/qa/qaspi0.log*

Windows: *%QASPI_Install_Dir%\log\qa\qaspi0.log*

Failed to delete the sites. Please check the log files.

Occurs when the NNM iSPI Performance for QA fails to delete the selected site configuration from the database.

Reason and Resolution

Check any of the following log files:

UNIX: *./var/opt/OV/log/qa/qaspi0.log*

Windows: *%QASPI_Install_Dir%\log\qa\qaspi0.log*

HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA) Threshold Configuration

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 avaiable 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)**[1] 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.

The threshold already has the possible settings. Cannot add more.

Occurs if you click Add **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 **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.

Add Threshold Settings form is closed. Cannot save the data.

Occurs when the Add Threshold Settings is closed before you saved the information.

Reason and Resolution

[1] The time required for a signal pulse or packet to travel from a specific source to a specific destination and back again.

You must save the information in the Add Threshold Settings form. Otherwise the threshold values for the selected source site, destination site, and the servive type are not reflected in the QA SPI database.

Metric field cannot be empty.

Occurs when you have not selected a metric in the Add Threshold Settings form.

Reason and Resolution

You must select the metric for the service type that you have selected in the Add Threshold Configuration.

Based on the metric you select you can select the high value, high value rearm, low value, and low value rearm for the metric.

High Value field cannot be empty.

Occurs when you try to save the information in Add Threshold Settings form without entering a high value for the metric.

Reason and Resolution

Based on the metric you select in the Add Threshold Settings form, the High Value, High Value Rearm, Low Value, or Low Value Rearm fields are enabled for the metric.

If the High Value and the High Value Rearm fields are enabled, and you have not set the high value for the metric, NNM iSPI Performance for QA does not have a threshold base to generate an incident if the metric value crosses the acceptable range.

If the High Value and the High Value Rearm fields are enabled, you must set at least the High Value for the metric. If you do not require the High Value Rearm value, enter 0(ZERO) for this field.

High Value Rearm field cannot be empty. Enter 0 if you do not have a high value rearm.

Occurs when you try to save the information in Add Threshold Settings form without entering a high value rearm for the metric.

Reason and Resolution

Based on the metric you select in the Add Threshold Settings form, the High Value, High Value Rearm, Low Value, or Low Value Rearm fields are enabled for the metric.

If the High Value Rearm field is enabled, and you have not set the high value rearm for the metric, NNM iSPI Performance for QA does not have a threshold base to cancel the incident generated when the metric crossed the high threshold value.

If the High Value Rearm field is enabled and you do not require the High Value Rearm value, enter 0(ZERO) for this field.

Low Value field cannot be empty.

Occurs when you try to save the information in Add Threshold Settings form without entering a low value for the metric.

Reason and Resolution

Based on the metric you select in the Add Threshold Settings form, the High Value, High Value Rearm, Low Value, or Low Value Rearm fields are enabled for the metric.

If the Low Value and the Low Value Rearm fields are enabled, and you have not set the low value for the metric, NNM iSPI Performance for QA does not have a threshold base to generate an incident if the metric value crosses the acceptable range.

If the Low Value and the Low Value Rearm fields are enabled, you must set at least the Low Value for the metric. If you do not require the Low Value Rearm value, enter 0(ZERO) for this field.

Low Value Rearm cannot be empty. Enter 0 if you do not have a low value rearm.

Occurs when you try to save the information in Add Threshold Settings form without entering a low value rearm for the metric.

Reason and Resolution

Based on the metric you select in the Add Threshold Settings form, the High Value, High Value Rearm, Low Value, or Low Value Rearm fields are enabled for the metric.

If the Low Value Rearm field is enabled, and you have not set the low value rearm for the metric, NNM iSPI Performance for QA does not have a threshold base to cancel the incident generated when the metric crossed the low threshold value.

If the Low Value Rearm field is enabled and you do not require the Low Value Rearm value, enter 0(ZERO) for this field.

Invalid input. Low Value Rearm for the threshold cannot be lower than the Low value.

Occurs if the low value rearm you entered is lower than the low value that you have entered for the selected metric.

Reason and Resolution

When the low value for a metric goes below the low value threshold, NNM iSPI Performance for QA generates an incident if you have selected the option in the Add Threshold Settings form. When the network performance improves and the metric value reaches the low value rearm, the NNM iSPI Performance for QA cancels the incident. Therefore, the low value rearm must be higher than the low value.

Please enter a numeric value.

Occurs when you enter any other character but a number in the in the High Value, High Value Rearm, Low Value, or Low Value Rearm field in the Add Threshold Settings form.

Reason and Resolution

These fields accept only numeric values.

Invalid input. High Value Rearm for the threshold cannot be greater than the High Value.

Occurs if the high value rearm you entered is higher than the high value that you have entered for the selected metric.

Reason and Resolution

When the high value for a metric goes above the high value threshold, NNM iSPI Performance for QA generates an incident if you have selected the option in the Add Threshold Settings form. When the network performance improves and the metric value reaches the high value rearm, the NNM iSPI Performance for QA cancels the incident. Therefore, the high value rearm must be lower than the high value.

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:

UNIX: *./var/opt/OV/log/qa/qaspi0.log*

Windows: *%QASPI_Install_Dir%\log\qa\qaspi0.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 to 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 ti at least one source site. You may or may not associate the thresold to a destination site.

Check any of the following log files:

UNIX: *./var/opt/OV/log/qa/qaspi0.log*

Windows: *%QASPI_Install_Dir%\log\qa\qaspi0.log*

Error in deleting the threshold configuration. Please check the log files.

Occurs when the NNM iSPI Performance for QA fails to delete the selected threshold configuration from the database.

Reason and Resolution

Check any of the following log files:

UNIX: *./var/opt/OV/log/qa/qaspi0.log*

Windows: *%QASPI_Install_Dir%\log\qa\qaspi0.log*

Use Case for HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA) Threshold Configuration

Module	HP Network Node Manager iSPI Performance for Quality

	Assurance Software (NNM iSPI Performance for QA) Threshold Configuration
Use Case Name	Configuring 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 NNMi Performance SPI for Quality Assurance Site Configuration form.

Initialization

1. Log on to HP Network Node Manager i-Suite Software (NNMi) console using a username and password with administrator privileges.
2. Click **Configuration**.

   The Configuration tab expands.
3. Select **Quality Assurance Threshold Configuration**

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:

1. Launch the Threshold Configuration form. See "Threshold Configuration Process" (on page 43).
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 elemenets 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
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 **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 opions:
   - Click Save and Close **Save and Close**.
   - Click **Save** and then click **Close**.
2. Close the Threshold Configuration form by selecting any of the following opions:
   - Click Save and Close **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 **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 HP Network Node Manager iSPI Performance for Quality Assurance Software (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 QAgenerates 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**.

GUIs Referenced

- Quality Assurance Threshold Configuration form
- Add Threshold Configuration form
- Add Threshold Settings form

System Interface

HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA) console

HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA) Help for Operators

NNM iSPI Performance for QA enables you to:

- Discover the QA probes configured in the network managed by the HP Network Node Manager i-Suite Software (NNMi).
- Analyze the outcome of each QA probe for past one day, one week, and one month.

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

- Not Managed
- Out of Service

NNM iSPI Performance for QA retrieves the network performance at the packet level using the following metrics:

- **Round Trip Time (RTT)**[1]
- **Jitter**[2]
- Packet loss (Can be from source to destination, destination to source, or two way.)

For information on metrics, see NNM iSPI Performance for QA Metrics in the *HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA) Reports Online Help*.

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

- **IP SLA**[3]
- DISMAN Ping using RFC 4560

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

Log on to the HP Network Node Manager i-Suite Software (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.

For more information on accessing the Quality Assurance workspaces, see Accessing the Quality Assurance Workspace.

[1] The time required for a signal pulse or packet to travel from a specific source to a specific destination and back again.

[2] Jitter is a measure of the variability over time of the latency across a network. A very low amount of jitter is important for real-time applications using voice and video. Jitter can be positive, negative, from source to destination, and from destination to source.

[3] Cisco IOS IP SLAs is a feature included in the Cisco IOS Software that can allow administrators the ability to Analyze IP Service Levels for IP applications and services. IP SLA's uses active traffic-monitoring technology to monitor continuous traffic on the network. Using IP SLAs, routers and switches perform periodic measurements. The exact number and type of available measurements depends on the IOS version.

For more information on accessing the Quality Assurance inventory view, see Accessing the QA Probes Inventory View.

Accessing the Quality Assurance Workspace

After you install HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA), a new workspace for Quality Assurance gets added to your HP Network Node Manager i-Suite Software (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 username 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-Suite Software (NNMi) Online Help* for more information

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

Managing the Quality Assurance Workspace

The following describes the tasks you can perform in the Quality Assurance workspace:

Task Options to Manage the Quality Assurance Workspace

Task Option	Description
Open	Opens the Details form for the selected QA probe.
Refresh	Retrieves the latest information from the database and displays the data in the QA Probes view.
Stop 5 min Periodic Refresh	By default, NNM iSPI Performance for QA refreshes the QA Probes view after every five minutes. Click this icon to stop the automatic refresh. You need to refresh the view manually until you click the Refresh icon again. Clicking the Refresh button sets the automatic refresh on again.

Task Option	Description
Show View in New Window	Opens the view in an independent window.
Sort the workspace	Click on a column heading to sort the workspace data based on that column. For more information on sorting the Quality Assurance workspace, see Sorting Data in the Quality Assurance Workspace.
Filter the workspace	Right click on a column to create a filter for the column. For more information on filtering the Quality Assurance workspace, see Filtering Data in the QA Probes View.
Quick View Tooltip	Displays the attributes of the selected object.
Restore Default Settings	Restores the default settings to sort the QA probes displayed in the view. By default the QA probes are sorted based on the Name column in an ascending order.
Restore Default Filters	Removes all the filters that you created on the QA Probes view. For more information on filtering the columns in the Quality Assurance workspace, see Filtering Data in the Quality Assurance Workspace.

Filtering Data in the QA Probes View

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

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

Filtering is enabled only for limited columns.

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	Lowest Value	Highest Value
Status	• Equals `<value>` • Not equals `<value>`	• Is Empty • Not Empty • Contains • Matches	No Status	Critical
Name	• Equals `<value>` • Not	• Is Empty • Not Empty	No lowest value	No highest value

	equals <value>			
Owner	• Equals <value> • Not equals <value>	• Is Empty • Not Empty	No lowest value	No highest value
Service	• Equals <value> • Not equals <value>	• Is Empty • Not Empty	ICMP Echo	UDP
Source Site	• Equals <value> • Not equals <value> • Is Empty • Not Empty	No disallowed filter	No lowest value	No highest value
Destination Site	• Equals <value> • Not equals <value> • Is Empty • Not Empty	No disallowed filter	No lowest value	No highest value
RTT	• Equals <value> • Not equals <value> • Is Empty • Not Empty	• Contains • Matches	0	n/a
Jitter	• Equals <value> • Not equals <value> • Is Empty • Not Empty	• Contains • Matches	0	n/a
Packet Loss	• Equals <value> • Not equals	• Contains • Matches	0	n/a

`<value>`

- Is Empty
- Not Empty

NNM iSPI Performance for QA enables you to create customized filters using the Create Filter utility.

You can use this utility only for the Status,RTT, Jitter, and Packet Loss columns.

To create a custom filter, follow these steps:

1. Right-click on the column heading for Status,RTT, Jitter, or Packet Loss columns and select **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 any or all of the specified values.

   Example

   You want to display those QA probes that has a high **Round Trip Time (RTT)**[1] or a high Packet Loss.

   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 will display the following types of QA probes:

   The QA probes that have a high RTT

   The QA probes that have a high packet loss

   The QA probes that have both high RTT and packet loss.

   Not Equals

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

   Example

   You want to display those QA probes that neither has a high **Round Trip Time (RTT)**[2] nor a high Packet Loss.

   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 will display only those QA probes that neither have high RTT nor high packet loss.
3. Select **Apply**.

Sorting Data in the QA Probes View

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

[1] The time required for a signal pulse or packet to travel from a specific source to a specific destination and back again.

[2] The time required for a signal pulse or packet to travel from a specific source to a specific destination and back again.

Sorting is enabled only for limited columns.

By default the workspace is sorted based on the Name column.

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

Note: Click the ↻ Restore Default Settings icon to sort the workspace based on the default column.

Accessing the QA Probes View

The QA Probes view displays all the QA probes configured in the **network elements**[1]. The QA probes are discovered by the HP Network Node Manager i-Suite Software (NNMi) polling process.

To launch the QA Probes view:

1. Log on to NNMi console using your username and password.
2. Click **Quality Assurance** in the Workspaces panel. The Quality Assurance tab expands, displaying the QA Probes view. cl ick the QA Probes view to display the QA probes discovered in your network.

The QA Probes view displays the following key attributes for each QA probe. Each QA probe displays information for a specific time interval.

Note: The default time interval for is 300 seconds, or 5 minutes.

Key Attributes of the QA Probes View

Attribute Name	Description
Status	The status that the QA probe returned. A QA probe may return any of the following

[1] Examples of network elements are; source node, destination node, QA probe name, QA probe type, source site, destination site, class of service, QA probe UUID, node UUID, etc.

Attribute Name	Description
	statuses : - Normal - Warning - Critical - Unknown - Disabled - Not Polled - Not in Service - No 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 HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA) recognizes are as follows: - **UDP Echo**[1] - **ICMP Echo**[2] - **UDP**[3] - **TCP Connect**[4] - **VoIP**[5]

[1] A UDP Echo is a server program that gives you an echo of a text string that you send using a UDP client.

[2] ICMP Echo is a method used to test whether a particular host is reachable across an IP network; it is also used to self test the network interface card of the computer, or as a latency test. It measures the round-trip time and records any packet loss, response packets received, the minimum, mean, maximum and the standard deviation of the round trip time.

[3] The User Datagram Protocol (UDP) is one of the core members of the Internet Protocol Suite. UDP service type in QA SPI uses the UDP protocol and provides jitter measurements. With UDP protocol, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths.

[4] TCP Connect scans a normal TCP connection to determine if a port is available. This scan method uses the same TCP handshake connection that every other TCP-based application uses on the network.

[5] Voice over Internet Protocol (VoIP) is a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks. VoIP converts an analog voice signal to digital format and compresses the signal into Internet protocol (IP) packets for transmission over the Internet.

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
RTT	The round-trip time used by the selected QA probe Displays the following threshold states for the metric: • High • Nominal • Low • Not Polled • Unavailable • Threshold Not Set
Jitter	The **delay**[2] variance for a data packet to reach the destination device or site Displays the following threshold states for the metric: • High • Nominal • Low • Not Polled • Unavailable • Threshold Not Set
PL (Packet Loss)	The percentage of packets that failed to arrive at the destination. Displays the following threshold states for the metric: • High • Nominal • Low • Not Polled • Unavailable

[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 gegraphic 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
	- Threshold Not Set

The RTT, Jitter, and PL columns display the most recent network performance states.

The following table describes these values:

QA Probe Performance States

State	Description
High	The metric crossed the High threshold value
Nominal	The metric was measured within healthy range, or no thresholds are being monitored.
Low	The metric crossed the Low threshold value
Not Polled	Indicates that this metric is intentionally not polled. Some of the possible reasons are: • Performance Monitoring is not enabled, because of current Communication Configuration settings in NNMi • The parent Node or Interface is set to Not Managed or Out of Service.
Unavailable	Unable to compute the metric or the computed value is outside of the valid range (0.00 - 100.00).

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

Launching the Forms

To launch the forms:

1. From the Left navigation panel, select the Quality Assurance Workspace and select a <QA> view; for example, Quality Assurance - > QA Probes view.
2. Click **Open** to view the detailed information about a specific QA probe. The form displays the information specific to the selected QA probe.

QA Probes Form

Displays the details for the selected QA probe and the configurations associated to it.

QA Probes Form: Left Panel

The left panel of the QA Probes 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 any of the following status: • No Status • Normal • Disabled • Unknown • Warning • Major • Critical
Name	Name of the selected QA probe For Cisco IP SLA 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. **Note:** The QA probe names cannot be blank.
Owner	Name of the QA probe owner
Service	Type of the QA probe Possible service types are: • **UDP Echo**[1] • **ICMP Echo**[2] • **UDP**[3] • **TCP Connect**[4]

[1] A UDP Echo is a server program that gives you an echo of a text string that you send using a UDP client.

[2] ICMP Echo is a method used to test whether a particular host is reachable across an IP network; it is also used to self test the network interface card of the computer, or as a latency test. It measures the round-trip time and records any packet loss, response packets received, the minimum, mean, maximum and the standard deviation of the round trip time.

[3] The User Datagram Protocol (UDP) is one of the core members of the Internet Protocol Suite. UDP service type in QA SPI uses the UDP protocol and provides jitter measurements. With UDP protocol, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths.

[4] TCP Connect scans a normal TCP connection to determine if a port is available. This scan method uses the same TCP handshake connection that every other TCP-based application uses on the network.

Attribute	Description
	• **VoIP**[1]
Admin Index	The unique index ID given for each QA probe Available only for Cisco IP SLA QA probes.

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
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 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 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 will wait for a response from the destination node before aborting the request
Frequency	Frequency for the QA probe in seconds
TOS	Type of Service specified in an IP packet header that indicates the service level required for the packet

[1] Voice over Internet Protocol (VoIP) is a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks. VoIP converts an analog voice signal to digital format and compresses the signal into Internet protocol (IP) packets for transmission over the Internet.

Attribute	Description
VRF	Virtual Routing and Forwarding (VRFs) tables defined on the source node. This fields 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
Management Mode	Whether the source node is managed or not Possible states are as follows: • Managed • Unmanaged • Unknown

Tests 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
- Jitter Configuration
- Status
- Conclusions
- Incidents

Viewing Source Interface for a QA Probe

HP Network Node Manager iSPI Performance for Quality Assurance Software (NNM iSPI Performance for QA) enables you to view source interfaces to the QA probes and analyze the traffic flows passing through the interface.

The NNM iSPI Performance for QAmaps the interface only if the HP Network Node Manager i-Suite Software (NNMi) 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 **IP SLA**[1] QA probes, specify the source IP address to the QA probe.
- For RFC 4560 QA probes, specify the source interface index when configuring the QA 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.

Consider this use case, the IP SLA Data Jitter or VoIP QA probe is configured on the edge router; the edge router is a multi homed with different ISPs. So the SLA metrics makes more sense when the right interface for sending traffic is picked. So the customer would configure the IP SLA test with specific interface. In this case the interface is stored in the DB and also dumped to perf spi for reporting.

Assume that there is a threshold violation and the customer wants to see all the TopN talkers , scoped by the interface. This is achieved because the interface is stored in perf spi and all reports is scoped by interface.

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

[1] Cisco IOS IP SLAs is a feature included in the Cisco IOS Software that can allow administrators the ability to Analyze IP Service Levels for IP applications and services. IP SLA's uses active traffic-monitoring technology to monitor continuous traffic on the network. Using IP SLAs, routers and switches perform periodic measurements. The exact number and type of available measurements depends on the IOS version.

Appendix A: Glossary Terms

C

Class of Service

Class of Service (CoS) is a way of managing traffic in a network by grouping similar types of traffic (for example, e-mail, streaming video, voice, large document file transfer) together and treating each type as a class with its own level of service priority. The priority value can be between 0 and 7 that can be used by Quality of Service (QoS) disciplines to differentiate traffic.

D

delay

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

H

High

The QA probe measure for the network element performance crossed the High threshold value.

I

ICMP

The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is chiefly used by networked computers' operating systems to send error messages—indicating, for instance, that a requested service is not available or that a host or router could not be reached.

ICMP Echo

ICMP Echo is a method used to test whether a particular host is reachable across an IP network; it is also used to self test the network interface card of the computer, or as a latency test. It measures the round-trip time and records any packet loss, response packets received, the minimum, mean, maximum and the standard deviation of the round trip time.

IP SLA

Cisco IOS IP SLAs is a feature included in the Cisco IOS Software that can allow administrators the ability to Analyze IP Service Levels for IP applications and services. IP SLA's uses active traffic-monitoring technology to monitor continuous traffic on the network. Using IP SLAs, routers and switches perform periodic measurements. The exact number and type of available measurements depends on the IOS version.

J

Jitter

Jitter is a measure of the variability over time of the latency across a network. A very low amount of jitter is important for real-time applications using voice and video. Jitter can be positive, negative, from source to destination, and from destination to source.

L

Low

The QA probe measure for the network element performance crossed the Low threshold value.

M

Mean Opinion Scores(MOS)

A measurement of the subjective quality of human speech, represented as a rating index. MOS is derived by taking the average of numerical scores given by juries to rate quality and using it as a quantitative indicator of system performance.

N

Negative Jitter

When the delay variance in sending the data packet from the source network element is less than the predefined inter-packet delay. For example, If packets are sent with 10 ms interval, negative jitter means they were received with less than 10 ms interval.

network element

Examples of network elements are; source node, destination node, QA probe name, QA probe type, source site, destination site, class of service, QA probe UUID, node UUID, etc.

network elements

Examples of network elements are; source node, destination node, QA probe name, QA probe type, source site, destination site, class of service, QA probe UUID, node UUID, etc.

Nominal

The QA probes measure for the network element performance was within healthy range, or no thresholds are being monitored.

Not Polled

Indicates that this network element is not polled intentionally.

O

ODBID

ODBID is a custom attribute that the HP Network Node Manager i-Series Software(NNMi) topology uses to integrate the NNMi topology with Business Service Management(BSM) software suite. The Smart Plug-Ins (SPIs) get this attribute from NNMi during the discovery and keep a reference. You can use ODBID as a report toplogy filter.

P

Positive Jitter

When the delay variance in sending the data packet from the source network element is more than the predefined inter-packet delay. For example, If packets are sent with 10 ms interval, positive jitter means they were received with more than 10 ms interval.

R

Round Trip Time (RTT)

The time required for a signal pulse or packet to travel from a specific source to a specific destination and back again.

S

Site

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

site rules

Configuration associated to a site are called site rules. For example Node Group, Ordering, Test Name Pattern, etc are the site rules that are used to configure a site. The rules are prioritized inherently. The Node Group rule has the highest priority, the IP Address rule the second highest priority. Test Name Pattern rule has the third highest priority while the VRF Name rule has the the lowest priority among these foure 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 the rules.

sites

A logical organization of networking devices. In the scope of enterprise networks, a site can be a logical grouping of networking devices generally situated in similar gegraphic 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.

standard IPv6 shorthand notation

IPv6 addresses are generally written in the form, hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:h In this full notation, pairs of IPv6 bytes are separated by a COLON and each byte in turns is represented as a pair of hexadecimal numbers. For example, E3D7:0000:0000:0000:51F4:9BC8 Shorthand notation in IPv6 removes these bytes with a zero values from the text representation, though the bytes still remain present in the actual network address). For example, E3D7::51F4:9BC8:C0A8:6420.

T

TCP Connect

TCP Connect scans a normal TCP connection to determine if a port is available. This scan method uses the same TCP handshake connection that every other TCP-based application uses on the network.

Two Way Jitter

The two way jitter is the average of the upstream positive, upstream negative, downstream positve, and downstream negative jitter.

U

UDP

The User Datagram Protocol (UDP) is one of the core members of the Internet Protocol Suite. UDP service type in QA SPI uses the UDP protocol and provides jitter measurements. With UDP protocol, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths.

UDP Echo

A UDP Echo is a server program that gives you an echo of a text string that you send using a UDP client.

Unavailable

Unable to compute the performance state of the network element, or the computed value is outside the valid range.

V

VoIP

Voice over Internet Protocol (VoIP) is a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks. VoIP converts an analog voice signal to digital format and compresses the signal into Internet protocol (IP) packets for transmission over the Internet.

VRF

Virtual Routing and Forwarding (VRFs) tables include the routing information that defines the Virtual Private Network (VPN) attached to a Provider Edge (PE) router. Each VRF is on a PE router. All PE routers containing VRFs relevant to the named VPN are grouped in one VPN. A VRF can only belong to a single VPN and is grouped on the basis of the Route Targets.

Appendix B: Index