HP Network Node Manager iSPI Performance for Quality Assurance Software

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

Software Version: 9.10

Online Help

Document Release Date: March 2011

Software Release Date: March 2011

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Oracle Technology — Notice of Restricted Rights

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

For the full Oracle license text, see the license-agreements directory on the NNM iSPI Performance for QA product DVD.

Copyright Notice

Trademark Notices

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

UNIX® is a registered trademark of The Open Group.

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.

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

Acknowledgements

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

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

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

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

Documentation Updates

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

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

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

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

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

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

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

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

Support

Visit the HP Software Support Online web site at:

http://www.hp.com/go/hpsoftwaresupport

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

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

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

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

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

To find more information about access levels, go to:

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

Disclaimer for PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format.

Note: Some topics do not convert properly to PDF, causing format problems. Some elements of online help are completely removed from the PDF version. Those problem topics can be successfully printed from within the online help.

Contents

HP Network Node Manager iSPI Performance for Quality Assurance Software Help for Administrators

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

- Discover the QA probes configured in the nodes managed by NNMi
- Configure QA probes
- Configure threshold for a Site or QA probe
- Monitor the network performance and view the threshold state of the metric in the NNMi console
- Analyze the outcome of each QA probe and generate reports upto a maximum period of 13 months

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

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

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

NNM iSPI Performance for QA enables to monitor the network performance for the devices that support the following MIBS:

- CISCO-RTTMON-MIB
- DISMAN-PING-MIB
- JNX-RPM-MIB

NNM iSPI Performance for QA supports the following vendor- specific technologies:

- CISCO IP SLA
- JUNIPER RPM
- Other vendors supporting the DISMAN Ping using RFC 4560

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

- UDP Echo
- ICMP Echo
- UDP
- TCP Connect
- VoIP

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

- Not Managed
- Out of Service

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

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

- NNM iSPI Performance for QA workspace: Access the QA Probes view to view the status and other details for the pre-configured QA probes on the nodes managed by NNMi. In addition, you can access the Threshold Exceptions Probes view, Critical Probes View, and Baseline Exceptions Probes View to view a specific set of QA probes. For more information on accessing the Quality Assurance workspace, see Accessing the Quality Assurance Workspace.
- Quality Assurance Configuration console: You can access the Quality Assurance Configuration Console from the Configuration workspace in NNMi to configure sites, threshold, discovery filters, and global manager. However, the following configuration tasks can be performed directly in the NNMi console:
  - Probe Configuration
  - Probe Maintenance
  - Configure Thresholds for Probes

Discovering QA Probes Using nmsqadisco.ovpl Command

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

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

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

Parameters

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

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

Configuring QA Probes Using nmsqaprobeconfig.ovpl Command

Usage of `nmsqaprobeconfig.ovpl` command to configure QA probes on a node with `icmp_echo` test type or service:

```
nmsqaprobeconfig.ovpl -u <username> -p <password> -c <write community string> -n <hostname> -da <destination address> -tn <test name> -fr <test frequency> -tt icmp_echo [-sa <source address>] [-si <source interface name>] [-sp <source port>] [-vn <VRF name>] [-tos <type of service>] [-lt <test life time>] [-to <test time out>] [-ps <packet size>] [-pn <number of packets> [-pd <inter packet delay>] [-ct <codec type>]
```

Usage of `nmsqaprobeconfig.ovpl` command to configure QA probes on a node with `udp_echo` or `udp`, or `tcp_connect` test type or service:

Note: Enter the test type as `udp_echo` or `udp` or `tcp_connect`

```
nmsqaprobeconfig.ovpl -u <username> -p <password> -c <write community string> -n <hostname> -da <destination address> -tn <test name> -fr <test frequency> -tt [udp_echo|tcp_connect|udp|] -dp <destination port> [-sa <source address>] [-si <source interface name>] [-sp <source port>] [-vn <VRF name>] [-tos <type of service>][-lt <test life time>] [-to <test time out>] [-ps <packet size>] [-pn <number of packets> [-pd <inter packet delay>] [-ct <codec type>]
```

Usage of `nmsqaprobeconfig.ovpl` command to configure QA probes on a node with `voip` test type or service:

```
nmsqaqaprobeconfig.ovpl -u <username> -p <password> -c <write community string> -n <hostname> -da <destination address> -tn <test name> -fr <test frequency> -tt voip -ct <Cdec Type> [-sa <source address>] [-si <source interface name>] [-sp <source port>] [-dp <destination port>] [-vn <VRF name>] [-tos <type of service>] [-lt <test life time>] [-to <test time out>] [-ps <packet size>] [-pn <number of packets>] [-pd <inter packet delay>] -ct <codec type>
```

Batch Upload of QA Probes Using Command Line Utility

Use the following command to to do a batch upload of a number of QA probes in NNM iSPI Performance for QA

`nmsqaprobeconfig.ovpl -u <username> -p <password> -f <` *qa probe setup input file*>

Note: You can find the input file format `qaprobeconfig.tmpl` in the following directory:

On UNIX: */var/opt/OV/shared/qa/conf*

On Windows: *%NnmDataDir%\shared\qa\conf*

This file gives you the format to enter the probe configuration details and upload the QA probes.

Note: While you enter probe configuration details for a specific test type or service type in the *qa probe setup input file*, the user needs to enter only those parameters that are required and delete the other parameters. However, you **must** specify the test name in the *qa probe setup input file* for all the test type or service type.

Parameters

- `-u <username>`: Type the username. This is a required parameter.
- `-p <password>`: Type the password. This is a required parameter.
- `-c <write community string>`: Type the write community string to use for authentication on the remote node. If you leave this field blank, the value is retrieved from NNMi.
- `-n <hostname>`: Type the hostname of the node. This is a required parameter.
- `-tn <test name>`:Type the name of the probe.This is a required parameter.
- `-tt <test type>`: Type the test type or service for which you intend to configure QA probes. The valid test types are `icmp_echo, udp_echo, tcp_connect, udp, and voip`. This is a required parameter.
- `-fr <test frequency>`: Type the frequency at which the specific QA probe test must be repeated in seconds. This is a required parameter.
- `-sa <source address>]`: Type the source address of the probe in the node.
- `-si <source interface name>`: Type the source interface name of the probe in the node.
- `-sp <source port>`: Type the source port of the probe in the node.
- `-da <destination address>`: Type the destination address of the node for which you intend to configure QA probes. This is a required parameter.
- `-dp <destination port>`: Type the destination port. This is a required parameter if you selected `udp_echo, tcp_connect, udp`, or `voip` service or test type.
- `-vn` <VRF name>:Type the name of the VRF.
- `-tos <type of service>`: Type the type of service.
- `-lt <test life time>`:: Type the life time of the probe in seconds.
- `-to <test time out>`: Type the maximum time the source node will wait for a response from the destination node before stopping the request in milliseconds.
- `-ps <packet size>`: Type the size of the packet sent.
- `-pn <number of packets>`: Type the number of packets sent.
- `-pd <inter packet delay>`: Type the inter packet delay in milliseconds.
- `-cn <codec number of packets>`: Type the number of codec packets you need to configure the QA probes.
- `-ct <CdecType>`: Type the codec type for which you need to configure the QA probes. The valid codec types are `g711_u_law` or `g711_a_law` or `g729a`. This is a required parameter if you selected the `voip` service.

The probes configured will be discovered in the next discovery cycle.

HP Network Node Manager iSPI Performance for Quality Assurance Software Quality Assurance Configuration Console

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

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

- Probe Configuration
- Probe Maintenance
- Configure Thresholds for Probes

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

Launching the Quality Assurance Configuration Console

To launch the Quality Assurance Configuration console:

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

   You must have administrator privileges.

2. From the workspace navigation panel, select the **Configuration** workspace.
3. Select **Quality Assurance Configuration Console**

   The Quality Assurance Configuration console opens.

   The following list of configuration links appear below the **Configuration** workspace in the left pane.

   - Site: You can configure sites for a global manager or a regional manager. By grouping the networking devices into sites, you can get an overview of the network performance
   - Site Based Threshold: You can configure thresholds for the existing sites
   - Probe Specific Threshold: You can view the list of QA probes for which you have configured the threshold, and you can edit the probe-specific threshold if required.
   - Discovery Filters: You can configure a discovery filter to exclude the QA probes based on some of the attributes of the QA probe
   - Global Network Management: You can configure the regional manager specific to NNM iSPI Performance for QA using this user interface in the global manager.

4. You can click on the required link in the left pane for configuration.

   The configuration summary details appear as follows:

a. **Site**

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

b. **Threshold**

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

c. **Discovery Filters**

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

d. **Global Network Management**

Field Name	Description
Regional Managers	Indicates the number of regional managers configured (if any) for the logged in NNMi management server

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

Icons Available in the Quality Assurance Configuration Toolbar	Description
 Close	Closes the Quality Assurance Configuration console

Icons Available in the Quality Assurance Configuration Toolbar	Description
 Refresh	Retrieves the last saved configuration details from the database, update the summary details and displays the data in the Quality Assurance Configuration console

Related Topics

Launch the Site Configuration Form

Launch the Threshold Configuration Form

Launch the Probe Specific Threshold Form

Launch the Discovery Filter Configuration Form

Launch the Global Network Management Configuration Form

HP Network Node Manager iSPI Performance for Quality Assurance Software Site Configuration

NNM iSPI Performance for QA enables you to monitor the network performance of different network elements . Logically grouping the networking devices into sites enables to monitor a similar set of QA probes.

Example

An enterprise network with branch offices is connected to the head office via WAN links. You can measure the network performances across all the offices and compare the network performance of the head office and the branch offices. This is useful to get an overview of health or the performance of the network.

You can configure QA probes between individual nodes or node groups and assign them to the sites. Also, you can configure the threshold for a site using the Threshold Configuration form. The threshold configured for a site is applied to all the QA probes of the site. This procedure takes very less time compared to configuring the threshold for each probe. You can view the measured value of the metrics for a site, which enables you to analyze the site and inter-site performance as well.

In a Global Network Management (GNM) environment, you can configure sites on a global manager or a regional manager. Based on this configuration, sites can be categorized as follows:

- Local Sites: Sites configured in the local NNMi management server are referred to as Local Sites. The local sites are owned by the manager on which it is configured.
- Remote Sites: The sites exported from the regional manager to the global manager are known as Remote Sites.

Whenever you create, edit, or delete a site in the regional manager, the changes are propagated to the global manager. You can export local sites, but you cannot export or delete remote sites. The advantage of exporting sites is that you need not configure the sites again.

Note: The sites configured and exported in the previous version of NNM iSPI Performance for QA can be imported and used in this version as well. See the topic Importing Sites Using Site Configuration Form for more information.

QA Probes Association

QA probes can be associated with either a local site or a remote site. Probes can be categorized as follows:

- Local QA Probes: Local QA probes are QA probes owned by the local manager.
- Remote QA Probes: Remote QA probes are primarily discovered and polled at the regional manager

  If a QA probe associated with the remote site matches the local site, the QA probes of the local site overrides the remote site QA probes. In such instances, NNM iSPI Performance for QA overrides the site configuration and not the thresholds configured for the site.

  However, if there is no local site that matches the remote site, the QA probes are associated with the remote site.

Example

Consider a network managed in a GNM environment with branch offices 1 and 2 monitored by regional managers R1 and R2 with the global manager as G1. Consider a set of sites configured in R1 and R2, which are exported to G1. The probes obtained from R1 and R2 are consolidated in G1.

If the sites matching the remote probes are configured in G1, the QA probes of G1 override the remote site QA probes. If there is no match, the remote QA probes are available in G1.

Related Topics

Launch the Site Configuration Form

Add a New Site

Edit an Existing Site

Delete an Existing Site

Delete All Existing Sites

Re-Computing Probes Associated to a Site

Export a Site Using Site Configuration Form

Import Sites Using Site Configuration Form

Launching the Site Configuration Form

Perform the following steps to launch the site configuration form:

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

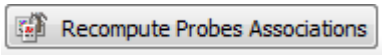
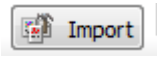
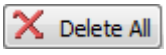
   You must have administrator privileges.
2. From the workspace navigation panel, select **Configuration** workspace.
3. Select **Quality Assurance Configuration Console**

The console opens.

4. In the **Configuration** workspace, select **Site**

   The Site Configuration form opens.

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

Icons 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	Saves the current configuration and closes the Site Configuration form
 Refresh	Retrieves the last saved site configuration from the database and displays the data in the Configured Sites panel of the Site Configuration form
 Recompute Probe Associations	Re-assigns the QA probes to the sites
 Export	Exports the existing sites
 Import	Imports sites from an XML file
Icons Available in the Global Settings Panel	**Description**
Enable Site Configuration	Enables to associate the configured sites to the probes
Icons Available in the Configured Sites Tab	**Description**
 New	Adds a new site
 Open	View an existing site
 Edit	Edits an existing site
 Delete	Deletes an existing site
 Refresh	Refreshes the Configured Sites panel and displays the last saved site configurations
 Delete All	Deletes all the existing sites

You can view the following in the **Configured Sites** panel:

Field Name	Description
Site Name	The name of the site configured.
Regional Manager	The regional manager where the sites are configured.
Ordering	The ordering number assigned to the site.
Node Group Rule	The node group rule configured for the site.
IP Range Rule	The IP range rule configured for the site.
Probe Name Rule	The probe name rule configured for the site.
VRF Name Rule	The VRF name rule configured for the site.

Related Topics

Overview of Site Configuration

Add a New Site

Edit an Existing Site

Delete an Existing Site

Delete All Existing Sites

Export a Site

Import 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:
   a. **Site Name**

      Enter the name you want to assign to the site.

      Site names are case sensitive. That is `SiteA` and `Sitea` are considered two different sites.

Site names must be unique. Also, it is recommended to use unique site names across the sites in a GNM environment.

Site names cannot contain ' (single quotation marks).

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

b. **Ordering**

A QA probe can be associated to only one source or destination site. Specify an ordering number for the site in this field to resolve conflicts in case a QA probe matches multiple sites. The NNM iSPI Performance for QA associates the QA probe with the site that has the lowest ordering number.

If you do not provide an ordering number for the site, the NNM iSPI Performance for QA assigns default ordering. Default ordering for a site is given the lowest priority.

The QA probe is associated with the site which has the **lowest** ordering in case the QA probe matches multiple sites.

Example 1

The discovered QA probe name "`UDP QA probe from Site A over WAN link to SiteB`" is associated 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 the QA probe — `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 are used to resolve the conflict. The weights are inherent to the site rules.

Example 2

The discovered QA probe name "`UDP QA probe from Site A over WAN link to SiteB`" is associated 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 Software and must be already present in the NNMi database.

d. **IP Address Range**

Type the IP address or IP address range and click 

Add to associate an IP address or IP address range to the site. The new IP address is added to the list in the IP Address Range box. You can add IPv4 and IPv6 addresses.

Select an IP address or IP address range and click 

Delete to remove it from the IP Address Range box.

You can click 

Delete All to remove all the addresses listed in the IP Address Range box.

Follow the rules 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.

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 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`" preceding any number of characters.

If you have two QA probes named "`UDP QA probe From SiteA over Provider WAN to SiteB`" and "`ICMP QA probe From SiteA over Provider WAN to SiteB`", NNM iSPI Performance for QA retrieves both QA probe names.

Example 2

QA Probe Name Pattern: `remote???|to|central*`

This QA probe pattern retrieves QA probe names that match the following criteria:

- The source information on the left hand side of the delimiter "`to`" should contain the string "`remote`", 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 "`remoteABC to centralHQ`", and "`remote123 to centralsite`, NNM iSPI Performance for QA retrieves both QA probe names.

- You cannot include blank spaces in QA probe name pattern, but you must enter the wild card "*" (asterisk) wherever required. See the example below:

Example 3

QA Probe Name Pattern: `*|to|Bangalore`

Note that "*" must be entered in the source information if you intend to leave the source information blank, and you want to retrieve the QA probe names of the destination, `Bangalore`. In this example, it does not check for the source information, and it retrieves all the probe name patterns with the destination information as `Bangalore`.

Select a QA probe name and click 

Delete to remove it from the Probe Name Patterns box.

You can click 

Delete All to select all the QA probes listed in the Probe Name Patterns box and remove them from the Probe Name Patterns box.

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 ranges. Make sure that the VRF name is associated with the IP address rule that is defined.

You can associate a different VRF range with the site. Type the VRF range and click Add **Add** to associate another VRF range to the site. The new VRF range is added to the list in the VRF Wildcards box.

You can specify a range of VRF using the wildcard character "**?**" (to replace one character) and "*****" (to replace multiple characters).

Select a VRF range and click Delete **Delete** to remove it from the VRF Wildcards box.

You can click Delete All **Delete All** to remove all the VRF ranges listed in the VRF Wildcards box.

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

Icons	Description
 Close	Closes the Add Site Configuration form without saving the site information you have entered
 Save	Saves the new site information
 Save and Close	Saves the site information and closes the Add Site Configuration form
 Clear	Clears the site information you have entered in the form

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

Related Topics

Overview of Site Configuration

Edit an Existing Site

View a Site

Delete an Existing Site

Delete All Existing Sites

Re-Computing Probes Associated to a Site

Export a Site

Import Sites

Editing an Existing Site Using the Site Configuration Form

To edit an existing site:

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

   The Edit Site Configuration form opens.

   Note: From the global manager, you can only view the remote sites, and you cannot edit the remote site details.
3. Update the following values as required:
   a. **Site Name**

      Enter the name you want to assign to the site.

      Site names are case sensitive. That is `SiteA` and `Sitea` are considered two different sites.

      Site names must be unique. Also, it is recommended to use unique site names across the sites in a GNM environment.

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

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

   b. **Ordering**

      A QA probe can be associated to only one source or destination site. Specify an ordering number for the site in this field to resolve conflicts in case a QA probe matches multiple sites. The NNM iSPI Performance for QA associates the QA probe with the site that has the lowest ordering number.

      If you do not provide an ordering number for the site, the NNM iSPI Performance for QA assigns default ordering. Default ordering for a site is given the lowest priority.

      The QA probe is associated with the site which has the **lowest** ordering in case the QA probe matches multiple sites.

      Example 1

      The discovered QA probe name "`UDP QA probe from Site A over WAN link to SiteB`" is associated 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 the QA probe — `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 are used to resolve the conflict. The weights are inherent to the site rules.

      Example 2

      The discovered QA probe name "`UDP QA probe from Site A over WAN link to SiteB`" is associated 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 assigns a site the lowest ordering value.

c. **Node Group**

Enter the node group that you want to assign to the site.

You can classify the node groups based on their types, geographic locations etc, while you add them to a site.

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

d. **IP Address Range**

Type the IP address or IP address range and click 

Add to associate an IP address or IP address range to the site. The new IP address is added to the list in the IP Address Range box. You can add IPv4 and IPv6 addresses.

Select an IP address or IP address range and click 

Delete to remove it from the IP Address Range box.

You can click 

Delete All to remove all the addresses listed in the IP Address Range box.

Follow the rules 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.

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 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`" preceding any number of characters.

If you have two QA probes named "`UDP QA probe From SiteA over Provider WAN to SiteB`" and "`ICMP QA probe From SiteA over Provider WAN to SiteB`", NNM iSPI Performance for QA retrieves both QA probe names.

Example 2

QA Probe Name Pattern: `remote???|to|central*`

This QA probe pattern retrieves QA probe names that match the following criteria:

- The source information on the left hand side of the delimiter "`to`" should contain the string "`remote`", 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 "`remoteABC to centralHQ`", and "`remote123 to centralsite`, NNM iSPI Performance for QA retrieves both QA probe names.

- You cannot include blank spaces in QA probe name pattern, but you must enter the wild card "*" (asterisk) wherever required. See the example below:

Example 3

QA Probe Name Pattern: `*|to|Bangalore`

Note that "*" must be entered in the source information if you intend to leave the source information blank, and you want to retrieve the QA probe names of the destination, `Bangalore`. In this example, it does not check for the source information, and it retrieves all the probe name patterns with the destination information as `Bangalore`.

Select a QA probe name and click Delete **Delete** to remove it from the Probe Name Patterns box.

You can click Delete All **Delete All** to select all the QA probes listed in the Probe Name Patterns box and remove them from the Probe Name Patterns box.

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 ranges. Make sure that the VRF name is associated with the IP address rule that is defined.

You can associate a different VRF range with the site. Type the VRF range and click Add **Add** to associate another VRF range to the site. The new VRF range is added to the list in the VRF Wildcards box.

You can specify a range of VRF using the wildcard character "**?**" (to replace one character) and "*****" (to replace multiple characters).

Select a VRF range and click Delete **Delete** to remove it from the VRF Wildcards box.

You can click Delete All **Delete All** to remove all the VRF ranges listed in the VRF Wildcards box.

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

Icons	Description
Close	Closes the Edit Site Configuration form without saving the site information you have entered
Save	Saves the new site information
Save and Close	Saves the site information and closes the Edit Site Configuration form
Clear	Clears the site information you have entered in the form

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

Related Topics

Overview of Site Configuration

Add a New Site

View a Site

Delete an Existing Site

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.

Note: In a GNM environment, the global manager cannot delete Remote Sites . The sites deleted at the regional manager are propagated to the global manager. In case, the synchronization takes more time, you can run the following commands to trigger synchronization:

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

```
nmsqasiteconfigutil synchronize <regional manager name>
```

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

```
nmsqasiteconfigutil synchronize all
```

Deleting All the Existing Sites Using the Site Configuration Form

To delete all the existing sites:

1. Launch the Site Configuration form.
2. Click  **Delete All**.
3. Click  **Refresh** in the **Configured Sites** panel to view the changes.

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

Note: In a GNM environment, the global manager cannot delete Remote Sites . The sites deleted at the regional manager are propagated to the global manager. In case, the synchronization takes more time, you can run the following commands to trigger synchronization:

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

```
nmsqasiteconfigutil synchronize <regional manager name>
```

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

```
nmsqasiteconfigutil synchronize all
```

Viewing an Existing Site Configuration Using the Site Configuration Form

To view a site configuration:

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

   The View Site Configuration Details form opens.

   You can view the following details:

Field Name	Description
Site Name	The name of the site.
Ordering	The ordering number for the site. This field displays "Default" if you have not specified a value for this field while creating the site.
Regional Manager	The name of the Regional Manager where the site was configured.
Node Group	The node group assigned to the site.
IP Address Range	The set of IPv4 or IPv6 addresses associated to the site.
Probe Name Pattern	The QA probes or the Probe Name patterns of the QA probes that are associated to the site.
VRF Wildcards	The VRF name associated to the site.

Related Topics

Overview of Site Configuration

Add a New Site

Edit an Existing Site

Delete an Existing Site

Delete All Existing Sites

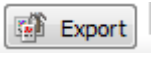
Re-Computing Probes Associated to a Site

Export a Site

Import Sites

Exporting a Site

To export the existing site configurations to an XML file:

1. Launch the Site Configuration form.
2. Click 

Export.

3. Enter the file name where you want to export the existing site configuration in the user prompt dialog.

   You must enter the file name with full path information; for example, `C:\temp\site_conf.xml`

   If you enter the XML file name without entering the absolute path, by default the file gets saved in the following directory of the NNMi management server where NNM iSPI Performance for QA is installed:

   UNIX: *$NnmDataDir/shared/qa/conf*

   Windows : *%NnmDataDir%\shared\qa\conf*

4. Click **OK** in the user prompt dialog.

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

UNIX: *$NnmInstallDir/bin/nmsqasiteconfigutil.ovpl –export [filename]*

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

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

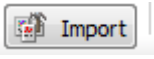
UNIX: *$NnmInstallDir/log/qa/qaspi0.log*

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

Note: You can export local sites, but you cannot export remote sites.

Importing Sites

To import site configurations from an XML file:

1. Launch the Site Configuration form.
2. Click 

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`

   Note: You can import the sites configured in the previous version of NNM iSPI Performance for QA as well.

4. Click **OK** in the user prompt dialog.

   If a site is already defined and displayed in the Configured Sites panel, the import utility does not import the configuration information for this site from the XML file.

You can also import site configuration information using the following command line utility:

UNIX: *$NnmInstallDir/bin/nmsqasiteconfigutil.ovpl –import [filename]*

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

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

UNIX:*$NnmInstallDir/log/qa/qaspi0.log*

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

Re-Computing Probes Associated to a Site

HP Network Node Manager iSPI Performance for Quality Assurance Software associates the QA probes with the respective sites during the configuration poll. However, if there are changes in the site configuration, the probes can be associated to the site by clicking on the Recompute Probes Associations button.

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*

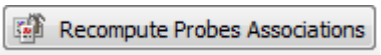
Also, the following VRF groups need to be added:

- 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 Probes 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:** *.$NnmInstallDir/bin/bin/nmsqasiteconfigutil.ovpl –recompute*
  - **Windows:** *%NnmInstallDir%\bin\nmsqasiteconfigutil.ovpl –recompute*

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

Note: In case, the recomputation does not occur due to an internal error, you can run the following command to reset the internal queue and the gateway flag to allow subsequent probe associations:

```
nmsqasiteconfigutil resetrecomputeQ
```

HP Network Node Manager iSPI Performance for Quality Assurance Software Site Wide Threshold Configuration

NNM iSPI Performance for QA thresholds enables you to track the health and performance of the network elements in a network.

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

To configure a threshold for a site, you must have a source site, but may not have a destination site. If you do not assign a destination site to the threshold, the threshold is applied to all the QA probes run from the source site.

You can configure thresholds for the following Quality Assurance metrics derived from the QA probes configured for an existing site:

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

NNM iSPI Performance for QA performs the following actions if a threshold is breached:

- Sets the QA probe status to Major.
- Creates an incident for the violated threshold.
- Sends the threshold violation details to the Network Performance Server for generating reports
- Retains the threshold state as Nominal, or sets the threshold state to High or Low depending on the count based, or time based threshold configuration

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

In a GNM environment, the global manager receives the threshold states from the sites in the regional managers. You **cannot** configure thresholds for remote sites. The thresholds configured for the sites of the global managers are not applicable for the sites of regional managers.

You can monitor the network performance and generate an incident based on the count based threshold or time based threshold configuration.

Note: You can only configure either a count based or time based threshold configuration for a combination of a site, service, and metric.

Threshold Configurations

Count Based Threshold Configuration

You can generate an incident based on the count or number of consecutive times a metric violates the threshold value. You can define this count in the Threshold Configuration form, and you can specify to trigger an incident when the threshold violation exceeds this count.

Time Based Threshold Configuration

Time based threshold configuration is useful when you intend to alert the user when the threshold breached state persists for more than a specific time period. This is derived by specifying X as the duration of time in minutes when the metric is in a threshold breached state within Y number of minutes specified in the sliding window. Based on your choice, you can trigger an incident if required.

Example for Time Based Threshold Configuration

Consider a scenario, where the polling interval is 5 minutes; High duration is 10 minutes; and High Duration Window is 60 minutes. In this scenario, an incident is generated whenever the High Duration exceeds 10 minutes within the 60 minute duration. NNM iSPI Performance for QA uses a sliding window wherein each time the High Duration (10 minutes) is reached, NNM iSPI Performance for QA drops the oldest polled value (first 5 minutes) and adds the most recent (between 60 to 65 minutes). This procedure continues and enables you to determine time based threshold violation.

You can make utmost use of the Time based threshold violation by ensuring that the duration specified in the sliding window is greater than or equal to the polling interval.

Baseline Settings Configuration

Baseline Deviation Settings Configuration

Apart from the time based and count based threshold configuration, you can also do a baseline monitoring based on the baseline deviation setting configuration in NNM iSPI Performance for QA. You can do a baseline deviation setting configuration for the selected site, service, and metric. An incident is generated and the baseline state transitions to Abnormal Range only if it meets all the criteria listed below:

- Exceeds the count or the number of standard deviation that is above the average value for the metric, or exceeds the count or the number of standard deviation that is below the average value for the metric.This count is specified in the Upper Baseline Limit Deviations or Lower Baseline Limit Deviations for the selected metric in the baseline deviation settings configuration.
- Exceeds the duration for which the upper or lower baseline deviation persists in the specified sliding window duration

Related Topics

Launch the Threshold Configuration Form

Add New Threshold Configuration to a Site

Edit Threshold Configuration of a Site

Delete an Existing Threshold of a Site

Delete All Existing Thresholds of a Site

Import Thresholds of a Site

Export Thresholds of a Site

Launching the Threshold Configuration Form

To launch the threshold configuration form:

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

   You must have administrator privileges.

2. From the workspace navigation panel, select **Configuration** workspace.

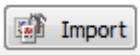
3. Select **Quality Assurance Configuration Console**.
   The console opens.

4. In the **Configuration** workspace, select **Site Based Threshold**

   The Threshold Configuration form opens.

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.

Icons Available in the Threshold Configuration Toolbar	Description
 Close	Closes the Threshold Configuration form without saving the current configuration
 Save	Saves the current configuration.
 Save and Close	Saves the current configuration and closes the Threshold Configuration form
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data in the Threshold Configuration form
 Export	Exports the existing thresholds
 Import	Imports thresholds from an XML file
Icons Available in the Global Settings Panel	**Description**
Enable	Enables the site wide threshold configuration
Icons Available in the Site Wide Configuration Panel	**Description**
 New	Adds a new threshold configuration
 Edit	Edits an existing threshold configuration
 Delete	Deletes an existing threshold configuration

Icons Available in the Threshold Configuration Toolbar	Description
 Refresh	Retrieves the last saved data from the database and displays the data in the Site Wide Configuration panel
 Delete All	Deletes all the existing thresholds

Related Topics

Overview of Threshold Configuration for Sites

Edit an Existing Threshold Setting of a Site

Delete an Existing Threshold of a Site

Delete All Existing Thresholds of a Site

Import Thresholds of a Site

Export Threshold of a Site

Adding New Threshold Configuration

To add a new threshold configuration:

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

   The Add Threshold Configuration form opens.
3. Specify the following information in the **Threshold Configuration** panel:

Field Name	Description
Source Site	Select the name of the source site. This field is mandatory.
Destination Site	Select the destination site for the QA probes. This field is optional.
Service	The type of the discovered QA probe. This field is mandatory. NNM iSPI Performance for QA recognizes the following QA probe types: ▪ UDP Echo ▪ ICMP Echo ▪ UDP ▪ TCP Connect

Field Name	Description
	▪ VoIP

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

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

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

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

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

Related Topics

Overview of Threshold Configuration for Sites

Edit Threshold Configuration of a Site

Delete an Existing Threshold of a Site

Delete All Existing Thresholds of a Site

Import Thresholds of a Site

Export Thresholds of a Site

Adding New Threshold Settings Using the Threshold Configuration Form

To add a new threshold:

1. Make sure that you selected the Source Site, and Service in the Add Threshold Configuration form if you are launching the form from Site Wide threshold configuration. You can ignore this step if you are launching this form from Probe based threshold configuration.
2. Click  **New** in the **Threshold Settings** tab.

   The Add Threshold Settings form opens.
3. Specify the following to configure the threshold settings:

Field Name	Description
Type	Select the type of threshold violation. The valid types are Count Based and Time Based.
Metric	Select the metric for which you are configuring the threshold. The metrics are populated based on the service.

4. After you select the metric to configure the threshold, the list of fields relevant to the selected metric appear. You can specify the following values to configure the new threshold:

Field Name	Description
High Value	Enter the threshold value. This value indicates the maximum value above which the metric will be considered to have violated the Nominal range. For Packet Loss metric, enter the High Value in percentage.
High Value Rearm	Enter the high rearm value for the threshold. For Packet Loss metric, enter the High Value Rearm in percentage. The High Rearm Value is used to indicate the end of the high threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value. The high value rearm must always be lower than the high value. **Example** For the Round Trip Time (RTT) you must generate an incident when the RTT is 150 and clear the incident when the RTT value comes down to 100. Set the following values for the threshold: ▪ High Value: `150` ▪ High Value Rearm: `100`

Field Name	Description
	This value enables you to be aware when a network performance problem starts to improve.
Low Value	Enter the low threshold value. This value indicates the maximum value below which the metric will be considered to have violated the Nominal range.
Low Value Rearm	Enter the low rearm value for the threshold. For Packet Loss metric, enter the Low Rearm Value in percentage. The Low Rearm Value is used to indicate the end of the low threshold state and NNM iSPI Performance for QA clears the incident once it reaches above this value. The low value rearm must be greater than the low value. **Example** For the Mean Opinion Score (MOS) you must generate an incident when the MOS score is 3 and clear the incident when the score is improved to 4.5. Set the following values for the threshold: ▪ Low Value: `3` ▪ Low Value Rearm: `4.5` This value enables you to be aware when a network performance problem starts to improve.

The following field appears, if you selected the Type as Count Based:

Field Name	Description
Trigger Count	Specify after how many consecutive threshold violations NNM iSPI Performance for QA must alert the operator by transitioning the threshold state to High or Low accordingly.

The following fields appear if you selected the Type as Time Based:

Field Name	Description
High Duration	The minimum duration for which the value must persist in a high value range for the threshold state to change to High and generate an incident (if specified). The polling interval must be less than or equal to the high duration value.
High Duration Window	The duration of the window within which the high duration

Field Name	Description
	criteria must be met. This value must be greater than 0 (zero), and this value can be the same as High Duration value. NNM iSPI Performance for QA uses a sliding window wherein each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polled value and adds the most recent.

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

Low Duration	The minimum duration for which the value must persist in a low value range for the threshold state to change to Low and generate an incident (if specified). The polling interval must be less than or equal to this low duration value.
Low Duration Window	The duration of the window within which the low duration criteria must be met. This value must be greater than 0 (zero), and this value can be the same as Low Duration value. NNM iSPI Performance for QA uses a sliding window wherein each time the Low Window Duration is reached, NNM iSPI Performance for QA drops the oldest polled value and adds the most recent.

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

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

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

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

7. Click **Refresh** to view the changes.
8. Click **Save** or **Save and Close** in the Threshold Configuration form.

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

NNM iSPI Performance for QA applies the following rules while creating thresholds for a **site** using this form:

- You can create thresholds only for the existing sites.
- You must select a source site and service for the new threshold.
- You could select the destination site for the new threshold
- If you do not specify a destination site for the threshold, the threshold is applied to all the destination sites of the source sites.
- You cannot configure thresholds for remote sites.

Note: For a Time Based Threshold configuration on probes, if the polling interval is greater than the High Duration or Low Duration value, the threshold cannot be configured for those QA probes. A list of these QA Probes, the UUID, and other details can be viewed in the log file, which is available in the following directory:

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

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

Related Topics

Overview of Threshold Configuration for Sites

Overview of Threshold Configuration for Probes

Adding New Baseline Settings Using the Threshold Configuration Form

To add a new baseline setting configuration:

2. 1. Make sure that you selected the Source Site, and Service in the Add Threshold Configuration form if you are launching the form from Site Wide threshold configuration. You can ignore this step if you are launching this form from Probe based threshold configuration.

   2. Click  **New** in the **Baseline Settings** tab.
   The Add Baseline Settings form opens.

   3. Specify the following to configure the baseline deviation settings:

      Note: You can expand or collapse the baseline deviation settings.

Field Name	Description
Metric	Select the metric for which you require to configure baseline deviation settings. The valid metrics for baseline deviation

Field Name	Description
	setting configuration are as below: ▪ RTT (ms) ▪ RTT (microS) ▪ Two Way Jitter (microS) ▪ Two Way Packet Loss (%) ▪ MOS

4. After you select the metric, the list of fields relevant to the selected metric appear. You can specify the following values to configure the baseline deviation settings:

Field Name	Description
Upper Baseline Limit Enabled	If you enable this option, NNM iSPI Performance for QA uses the Upper Baseline Limit Deviations-Above Average field value to determine the number of times there is a standard deviation above the average value. If you disable this option NNM iSPI Performance for QA does not consider the Upper Baseline Limit Deviations-Above Average field value. This field is not relevant and does not appear for MOS metric.
Upper Baseline Limit Deviations - Above Average	The number or count of standard deviation above the average values for NNM iSPI Performance for QA to determine the upper baseline limit. This field is not relevant and does not appear for MOS metric.
Lower Baseline Limit Enabled	If you enable this option, NNM iSPI Performance for QA uses the Lower Baseline Limit Deviations-Below Average field value to determine the number of times there is a standard deviation below the average value. If you disable this option NNM iSPI Performance for QA does not consider the Lower Baseline Limit Deviations - Below Average field value. This field appears only for MOS metric.
Lower Baseline Limit Deviations - Below Average	The number or count of standard deviation below the average values for NNM iSPI Performance for QA to determine the lower baseline limit. This field appears only for MOS metric.
Duration	The minimum time for which the standard deviation must persist to deviate from the configured Baseline Range before the baseline state transitions to Abnormal Range and generates an incident.

Field Name	Description
	The Polling Interval should be less than or equal to the Duration.
Window Duration	The window duration within which the Upper Baseline Limit or Lower Baseline Limit Deviation criteria must be met. The value must be greater than 0 (zero) and can be the same as the Duration value. NNM iSPI Performance for QA uses a sliding window, meaning that each time the Duration is reached, NNM iSPI Performance for QA drops the oldest polling cycle and adds the most recent.

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

Icons	Description
 Close	Closes the Add Baseline Settings form without saving the baseline setting information you have entered.
 Save and Close	Saves the baseline setting information and closes the Add Baseline Settings form

6. Click  **Save and Close** in the Add Baseline Settings form to save the baseline setting information.

7. Click  **Save** or  **Save and Close** in the Threshold Configuration form.

   Caution: The new baseline settings configuration is not saved unless you click  **Save** or  **Save and Close** in the Threshold Configuration form.

   NNM iSPI Performance for QA applies the following rules while configuring baseline deviation settings for a **site** using this form:

   - You can configure baseline settings only for the QA probes of the existing sites.
   - You must select a source site, service, and metric to configure the baseline settings.
   - Optionally, you can select the destination site
   - If you do not specify a destination site for the baseline setting, the configuration is applied to all the QA probes of the destination sites from the source sites.
   - You cannot configure baseline settings for remote sites.

Related Topics

Overview of Threshold Configuration for Sites

Overview of Threshold Configuration for QA Probes

Editing Threshold Configuration

To edit a threshold configuration:

1. Launch the Threshold Configuration form.
2. Select one or more site wide configuration and click  **Edit** in the **Site Wide Configuration** panel.

   The Edit Threshold Configuration form opens.
3. Specify the following information in the **Threshold Configuration** panel:

Field Name	Description
Source Site	Select the name of the source site. This field is mandatory.
Destination Site	Select the destination site for the QA probes. This field is optional.
Service	The type of the discovered QA probe. This field is mandatory. NNM iSPI Performance for QA recognizes the following QA probe types: ▪ UDP Echo ▪ ICMP Echo ▪ UDP ▪ TCP Connect ▪ VoIP

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

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

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

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

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

Related Topics

Overview of Threshold Configuration for Sites

Add New Threshold Configuration

Delete an Existing Threshold of a Site

Delete All Existing Thresholds of a Site

Import Threshold of a Site

Export Threshold of a Site

Editing an Existing Threshold Setting Using the Threshold Configuration Form

To edit an existing threshold setting:

1. Make sure that you selected the Source Site, and Service in the Edit Threshold Configuration form if you are launching the form from Site Wide threshold configuration. You can ignore this step if you are launching this form from Probe based threshold configuration in the NNMi console or the Probe Specific Thresholds Form in the Quality Assurance Configuration console.
2. Click on the **Threshold Settings** tab.
3. Select the threshold setting to be modified, and click  **Edit**.

   The Edit Threshold Settings form opens.

   You can view the threshold setting that was configured earlier.

   Note: For probe based threshold configuration, you can view the threshold that was configured for the Remote QA probes, but you **cannot** configure thresholds for Remote QA Probes.

   You cannot modify the following details:

Field Name	Description
Type	The type of threshold violation can be Count Based or Time Based.
Metric	The name of the metric.

4. You can modify the following information:

Field Name	Description
High Value	Enter the threshold value. This value indicates the maximum value above which the metric will be considered to have violated the Nominal range. For Packet Loss metric, enter the High Value in percentage.
High Value Rearm	Enter the high rearm value for the threshold. For Packet Loss metric, enter the High Value Rearm in percentage. The High Rearm Value is used to indicate the end of the high threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value. The high value rearm must always be lower than the high value. **Example** For the Round Trip Time (RTT) you must generate an incident when the RTT is 150 and clear the incident when the RTT value comes down to 100. Set the following values for the threshold: ▪ High Value: `150` ▪ High Value Rearm: `100`

Field Name	Description
	This value enables you to be aware when a network performance problem starts to improve.
Low Value	Enter the low threshold value. This value indicates the maximum value below which the metric will be considered to have violated the Nominal range.
Low Value Rearm	Enter the low rearm value for the threshold. For Packet Loss metric, enter the Low Rearm Value in percentage. The Low Rearm Value is used to indicate the end of the low threshold state and NNM iSPI Performance for QA clears the incident once it reaches above this value. The low value rearm must be greater than the low value. **Example** For the Mean Opinion Score (MOS) you must generate an incident when the MOS score is 3 and clear the incident when the score is improved to 4.5. Set the following values for the threshold: ▪ Low Value: `3` ▪ Low Value Rearm: `4.5` This value enables you to be aware when a network performance problem starts to improve.

The following fields appear, if the Type is Count Based, and you can modify the information if required

Field Name	Description
Trigger Count	Specify after how many consecutive threshold violations NNM iSPI Performance for QA must alert the operator by transitioning the threshold state to High or Low accordingly.

The following fields appear if the Type is Time Based, and you can modify the information if required:

Field Name	Description
High Duration	The minimum duration for which the value must persist in a high value range for the threshold state to change to High and generate an incident (if specified) The polling interval must be less than or equal to the high duration value.

Field Name	Description
High Duration Window	The duration of the window within which the high duration criteria must be met. This value must be greater than 0 (zero), and this value can be the same as High Duration value. NNM iSPI Performance for QA uses a sliding window wherein each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polled value and adds the most recent.

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

Note: You can modify the information if required.

Low Duration	The minimum duration for which the value must persist in a low value range for the threshold state to change to Low and generate an incident (if specified). The polling interval must be less than or equal to this low duration value.
Low Duration Window	The duration of the window within which the low duration criteria must be met. This value must be greater than 0 (zero), and this value can be the same as Low Duration value. NNM iSPI Performance for QA uses a sliding window wherein each time the Low Window Duration is reached, NNM iSPI Performance for QA drops the oldest polled value and adds the most recent.

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

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

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

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

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

8. Click  **Save and Close**.

   The Threshold Configurations form closes.

9. Click  **Save** or  **Save and Close** in the Threshold Configuration form.

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

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

- You can define thresholds only for the existing sites.
- Any modification in the threshold directly updates the state poller.

Note: For a Time Based Threshold configuration on probes, if the polling interval is greater than the High Duration or Low Duration value, the threshold cannot be configured for those QA probes. A list of these QA Probes, the UUID, and other details can be viewed in the log file, which is available in the following directory:

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

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

Related Topics

Overview of Threshold Configuration for Sites

Overview of Threshold Configuration for Probes

Editing Baseline Settings Using the Threshold Configuration Form

To edit a baseline setting configuration:

1. Make sure that you selected the Source Site, and Service in the Edit Threshold Configuration form if you are launching the form from Site Wide threshold configuration. You can ignore this step if you are launching this form from Probe based threshold configuration.
2. Select the baseline settings, and click  **Edit** in the **Baseline Settings** panel.

   The Edit Baseline Settings form opens.
3. To edit the baseline deviations settings in the **Baseline Deviations Settings** panel:

a. You can view the following details:

Field Name	Description
Metric	The metric for which you require to edit the baseline deviations settings configuration.

b. You can edit the following baseline deviation settings configuration:

Note: The following fields appear depending on the metric:

Field Name	Description
Upper Baseline Limit Enabled	If you enable this option, NNM iSPI Performance for QA uses the Upper Baseline Limit Deviations-Above Average field value to determine the number of times there is a standard deviation above the average value. If you disable this option NNM iSPI Performance for QA does not consider the Upper Baseline Limit Deviations-Above Average field value. This field is not relevant and does not appear for MOS metric.
Upper Baseline Limit Deviations - Above Average	The number or count of standard deviation above the average values for NNM iSPI Performance for QA to determine the upper baseline limit. This field is not relevant and does not appear for MOS metric.
Lower Baseline Limit Enabled	If you enable this option, NNM iSPI Performance for QA uses the Lower Baseline Limit Deviations-Below Average field value to determine the number of times there is a standard deviation below the average value. If you disable this option NNM iSPI Performance for QA does not consider the Lower Baseline Limit Deviations - Below Average field value. This field appears only for MOS metric.
Lower Baseline Limit Deviations - Below Average	The number or count of standard deviation below the average values for NNM iSPI Performance for QA to determine the lower baseline limit. This field appears only for MOS metric.
Duration	The minimum time for which the standard deviation must persist to deviate from the configured Baseline Range before the baseline state transitions to Abnormal Range and generates an incident.

Field Name	Description
	The Polling Interval should be less than or equal to the Duration.
Window Duration	The window duration within which the Upper Baseline Limit or Lower Baseline Limit Deviation criteria must be met. The value must be greater than 0 (zero) and can be the same as the Duration value. NNM iSPI Performance for QA uses a sliding window, meaning that each time the Duration is reached, NNM iSPI Performance for QA drops the oldest polling cycle and adds the most recent.

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

Icons	Description
 Close	Closes the Edit Baseline Settings form without saving the baseline setting information you have entered.
 Save and Close	Saves the baseline setting information and closes the Edit Baseline Settings form

5. Click  **Save and Close** in the Edit Baseline Settings form to save the baseline setting information.
6. Click  **Save** or  **Save and Close** in the Site Wide Threshold Configuration form.

Caution: The new baseline settings configuration is not be saved unless you click  **Save** or  **Save and Close** in the Threshold Configuration form.

NNM iSPI Performance for QA applies the following rules while configuring baseline deviation settings for a **site** using this form:

- You can configure baseline settings only for the QA probes of the existing sites.
- You must select a source site and service to configure the baseline settings.
- Optionally, you could select the destination site
- If you do not specify a destination site for the baseline setting, the configuration is applied to all the QA probes of the destination sites from the source sites.
- You cannot configure baseline settings for remote sites.

Related Topics

Overview of Threshold Configuration for Sites

Overview of Threshold Configuration for QA Probes

Deleting an Existing Threshold Using the Threshold Configuration Form

To delete an existing threshold:

1. Launch the Threshold Configuration form.
2. Select a threshold in the **Threshold Settings** panel and click **Delete**.
3. Click **Refresh** in the Threshold Settings panel to view the changes.

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

The selected thresholds configured for the metrics of the site are deleted and the threshold state is set to Threshold Not Set for the metric in the site. If any probe based configuration exists for the metric, the deletion of the site based threshold configuration has no impact on the probe based threshold configuration. The QA Probe status for the probes in the site is set to the most severe status. The incidents and conclusions are updated accordingly.

Example 1

Consider the following scenario:

Before Deleting the Threshold(s) Configured for the Site:

QA Probe Status : Major

Threshold State: High

Note: The threshold state is high for RTT and Packet Loss

Conclusion: RttThresholdStateHigh, TwoWayPktLossThresholdStateHigh, RTTAbnormal

After Deleting the Threshold(s) Configured for the Site:

QA Probe Status : Major

Threshold State: Threshold Not Set

Note:The threshold state is set to Threshold Not Set for RTT and Packet Loss.

Conclusion: RTTAbnormal

Note: The QA Probe Status for the probes in the site is still set to Major as the Baseline State is in the Abnormal Range.

Example 2

Consider the following scenario:

Before Deleting the Threshold(s) Configured for the Site:

QA Probe Status : Major

Threshold State: High

Conclusion: TestUp When both Administrative and Operational states are up., RttThresholdStateHigh,TwoWayPktLossThresholdStateHigh

After Deleting the Threshold(s) Configured for the Site:

QA Probe Status : Normal

Threshold State: Threshold Not Set

Conclusion: TestUp When both Administrative and Operational states are up.

Deleting All Existing Thresholds Using the Threshold Configuration Form

To delete all the existing thresholds:

1. Launch the Threshold Configuration form.
2. Click 

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

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

The thresholds configured for the site is deleted and the threshold state is set to Threshold Not Set for the probes in the site for which you have not configured a probe based threshold configuration. The Probe status of the QA probes in the site is set to the most severe status. The incidents and conclusions are updated accordingly.

Example 1

Consider the following scenario:

Before Deleting all the Thresholds Configured for the Site

QA Probe Status : Major

Threshold State: High

Note: The threshold state is high for RTT and Packet Loss

Conclusion: RttThresholdStateHigh, TwoWayPktLossThresholdStateHigh, RTTAbnormal

After Deleting all the Thresholds Configured for the Site:

QA Probe Status : Major

Threshold State: Threshold Not Set

Note: The threshold state is set to Threshold Not Set for RTT and Packet Loss.

Conclusion: RTTAbnormal

Note: The QA Probe Status of the probes in the site is still set to Major as the Baseline State is in the Abnormal Range.

Example 2

Consider the following scenario:

Before Deleting all the Thresholds Configured for the Site

QA Probe Status : Major

Threshold State: High

Conclusion: TestUp When both Administrative and Operational states are up., RttThresholdStateHigh,TwoWayPktLossThresholdStateHigh

After Deleting all the Thresholds Configured for the Site:

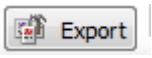
QA Probe Status : Normal

Threshold State: Threshold Not Set

Conclusion: TestUp When both Administrative and Operational states are up.

Exporting a Threshold

To export the existing threshold configurations to an XML file:

1. Launch the Threshold Configuration form.
2. Click 

Export.
3. Type the file name where you want to export the existing threshold configuration in the user prompt dialog.

   You must type the file name with full path information; for example, `C:\temp\threshold_conf.xml`

   If you type the XML file name without entering the absolute path, by default the file gets saved in the following directory:

   UNIX: *$NnmDataDir/shared/qa/conf*

   Windows : *%NnmDataDir%\shared\qa\conf*
4. Click **OK** in the user prompt dialog.

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

UNIX: *$NnmInstallDir/bin/nmsqathresholdconfigutil.ovpl –export [filename]*

Windows: *%NnmInstallDir%\bin\nmsqathresholdconfigutil.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: *$NnmInstallDir/log/qa/qaspi0.log*

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

Importing Thresholds

To import threshold configurations from an XML file:

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: *$NnmInstallDir/bin/nmsqathresholdconfigutil.ovpl –import [filename]*

Windows: *%NnmInstallDir%\bin\nmsqathresholdconfigutil.ovpl –import [filename]*

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

UNIX: *$NnmInstallDir/log/qa/qaspi0.log*

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

Launching the Probe Specific Threshold Form

To launch the probe specific threshold configuration form:

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

   You must have administrator privileges.

2. From the workspace navigation panel, select **Configuration** workspace.

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

   The console opens.

4. In the **Configuration** workspace, select **Probe Specific Threshold**.

   The Probe Specific Threshold form opens.

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

   You can view the following:

Attribute Name	Description
Name	The name of the discovered QA probe configured in the network device
Service	The type of the discovered QA probe Some of the QA probe types that the HP Network Node Manager iSPI Performance for Quality Assurance Software recognizes are as follows: ▪ UDP Echo ▪ ICMP Echo ▪ UDP ▪ TCP Connect

Attribute Name	Description
	▪ VoIP
Owner	The name of the discovered QA probe's owner.
Source	The source device from which the probe is configured.
Destination	The destination network device to which the probe is configured.
ToS	Type of Service specified in an IP packet header that indicates the service level required for the packet
Settings	Move the mouse over this icon to view a snapshot of all the threshold settings configured for the probe.

5. You can perform the following tasks using the Probe Specific Threshold Configuration form:

Icons Available in the Probe Specific Threshold Toolbar	Description
Close	Closes the Threshold Configuration form without saving the current configuration
Icons Available in the Probes With Specific Thresholds Tab	**Description**
Edit Configured Settings	Edits the selected probe based threshold configuration
Delete Configured Settings	Deletes an existing probe based threshold configuration
Refresh	Retrieves the last saved data from the database and displays the data in the view

Related Topics

Configure Threshold for QA Probes

Editing an Existing Threshold Setting

HP Network Node Manager iSPI Performance for Quality Assurance Software Discovery Filter Configuration

You may have numerous probes configured in your entire network. Not all these QA probes are always useful for you to analyze, monitor, or measure the network performance. So, you can restrict to discover, and monitor only a required set of probes in a network environment.

This feature allows you to exclude the QA probes (like the interface health reporting QA probes) that produces a lot of output, which may not be required for monitoring the network performance.

The Discovery Filter Configuration enables you to filter the discovery process, and exclude the QA probes based on the following attributes of the QA probe:

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

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

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

You can set three types of discovery filters in a Global Network Management environment, which are as follows:

- Discovery filter is selected to exclude the QA probes discovered on the network
- Regional Data Forwarding filter is configured in the regional manager and excludes the QA probes forwarded to the global manager
- Global Receiver filter is configured in the global manager and excludes the QA probes received by the global manager

Note: If you add a Regional Data Forwarding filter and a Global Receiver filter, both the discovery filters will be applied on the QA probes in the global manager.

Example

Consider a network managed in Global Network Management environment with branch offices 1 and 2 monitored by regional managers R1 and R2 with the global manager as G1. You can set the following filters:

- Set a discovery filter on R1 and R2 to exclude the QA probes discovered on the network. For example, you can create a discovery filter by selecting the Source IP address as 192.168.*.* . The QA probes with source IP address as 192.168.*.* will not be discovered in the network
- Set a Regional Data Forwarding filter at R1 and R2 to exclude the QA probes that must not be forwarded to G1. For example, you can create a Regional Data Forwarding filter by selecting the ICMP echo service. The QA probes of ICMP echo service will not be forwarded to the global manager.
- Set a Global Receiver filter at G1 to exclude the QA probes received by the global manager. For example, you can create a Global Receiver filter by selecting UDP echo service. The QA probes of UDP echo service will not be discovered at the global manager.

Related Topics

Launch the Discovery Filter Configuration Form

Add a New Discovery Filter

Edit a Discovery Filter

Delete an Existing Discovery Filter

Launching the Discovery Filter Configuration Form

To launch the discovery filter configuration:

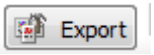
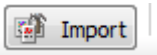
1. Log on to NNMi console using your username and password.

   You must have administrator privileges.
2. Select **Configuration** workspace.
3. Select **Quality Assurance Configuration Console**

   The console opens.
4. In the **Configuration** workspace, select **Discovery Filters**

   The Discovery Filter Configuration form opens.

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

Icons 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	Saves the current configuration and closes the Discovery Filter Configuration form
 Refresh	Retrieves the last saved discovery filter configuration from the database
 Apply Filter Now	Applies the discovery filters and deletes the filtered local QA Probes from the database. This functionality is applicable only for Local QA Probes and Discovery filter type.
 Export	Exports the existing discovery filter configuration
 Import	Imports discovery filter configuration from an XML file

Icons Available in the Global Settings Panel	Description
Enable Discovery Filters	Enables you to configure filters. If this option is not selected, you will not be able to use the Configured Filters panel.

Icons Available in the Configured Filters Tab	Description

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

Related Topics

Overview of Discovery Filter Configuration

Add a New Discovery Filter

Edit a Discovery Filter

Import Discovery Filters

Export a Discovery Filter

Delete an Existing Discovery Filter

Delete All Existing Discovery Filters

Adding a New Discovery Filter Using the Discovery Filter Configuration Form

To add a new discovery filter:

1. Launch the Discovery Filter Configuration form.
2. Select the **Enable Discovery Filters** option to activate the discovery filters.
3. Click  **New** in the **Configured Filters** panel in the Discovery Filter Configuration form.

   The Add Discovery Filter form opens.
4. Enter the following:

   a. **Name**

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

   b. **Type**

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

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

c. **Owner Names**

Type the QA probe owner name or a pattern suggesting the owner name to be filtered in the Owner Names box .
You can specify a range of QA probe owner names using the wildcard character **?** (to replace one character) and ***** (to replace multiple characters).
Click Add Add. The new QA probe owner name is added to the list in the Owner Names box.
You can select a QA probe owner name, and click Delete to remove it from the Owner Names box.
You can click Delete All **Delete All** to select all the QA probe owner names listed in the Owner Names box and remove them.

d. **Source IP Addresses**

Type the Source IP address or IP address range to be filtered and click Add **Add**. You can add IPv4 and IPv6 addresses. If the Source IP Address is not configured, you can enter the Management IP Address.
Select a Source IP address or IP address range and click Delete **Delete** to remove it from the Source IP Addresses box.
You can click Delete All **Delete All** to remove all the IP addresses listed in the Source IP Addresses box.

Follow the rules 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.

e. **Destination IP Addresses**

Type the Destination IP address or IP address range to be filtered and click Add **Add**. You can add IPv4 and IPv6 addresses.

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

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

Follow the rules 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.

f. **Service**

Select any one or more of the following services to be filtered and click Add **Add**

- UDP Echo
- ICMP Echo
- UDP
- TCP Connect
- VoIP

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

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

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

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

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

Icons	Description
 Close	Closes the Discovery Filter Configuration form without saving the filter information you have entered.

Icons	Description
 Save	Saves the new discovery filter information
 Save and Close	Saves the discovery filter information and closes the Discovery Filter Configuration form

Related Topics

Overview of Discovery Filter Configuration

Edit a Discovery Filter

Import a Discovery Filter

Export a Discovery Filter

Delete an Existing Discovery Filter

Delete All Existing Discovery Filters

Editing a Discovery Filter Using the Discovery Filter Configuration Form

To edit a discovery filter:

1. Launch the Discovery Filter Configuration form .
2. Select a filter in the in the **Configured Filters** tab in the Discovery Filter Configuration Form, and click  **Edit**.

   The Edit Discovery Filter form opens.
3. Select **Enable Discovery Filters** option to activate the discovery filters.
4. Update the following values as required:

   Note: You cannot edit the discovery filters configured for the regional managers from the global manager.

   a. **Name**

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

   b. **Type**

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

   - Discovery: Select this option to **exclude** the QA probes discovered on the network
   - Regional Data Forwarding: Select this option to **exclude** the QA probes forwarded to the

global manager

- Global Receiver: Select this option to **exclude** the QA probes received by the global manager. This option appears only for global manager.

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

c. **Owner Names**

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

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

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

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

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

d. **Source IP Addresses**

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

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

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

Follow the rules as discussed below, while defining a Source 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

e. **Destination IP Addresses**

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

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

Follow the rules 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

f. **Service**

Select any one or more of the following services to be filtered from the drop-down list, and click Add **Add**

- UDP Echo
- ICMP Echo
- UDP
- TCP Connect
- VoIP

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

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

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

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

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

Icons	Description
Close	Closes the Discovery Filter Configuration form without saving the filter information you have entered
Save	Saves the new discovery filter information

Icons	Description
 Save and Close	Saves the discovery filter information and closes the Discovery Filter Configuration form

Related Topics

Overview of Discovery Filter Configuration

Add a New Discovery Filter

Import a Discovery Filter

Export a Discovery Filter

Delete an Existing Discovery Filter

Delete All Existing Discovery Filters

Deleting an Existing Discovery Filter Using the Discovery Filter Configuration Form

To delete an existing discovery filter:

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

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

Deleting All Existing Discovery Filters Using the Discovery Filter Configuration Form

To delete all the existing discovery filters:

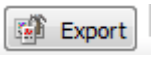
1. Launch the Discovery Filter Configuration form.
2. Click 

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

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

Exporting a Discovery Filter

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

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

Export.
3. Enter the file name where you want to export the existing discovery filter configuration in the user prompt dialog.

   You must enter the file name with full path information; for example, `C:\temp\disco_filter_conf.xml`

   If you enter the XML file name without entering the absolute path, by default the file gets saved in the following directory:

   UNIX: *$NnmDataDir/shared/qa/conf*

   Windows: *%NnmDataDir%\shared\qa\conf*
4. Click **OK** in the user prompt dialog.

You can also export the existing discovery filter using the following command line utility:

UNIX: *$NnmInstallDir/bin/nmsqadiscofilter.ovpl –export [filename]*

Windows: *%NnmInstallDir%\bin\nmsqadiscofilter.ovpl.ovpl –export [filename]*

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

UNIX: *$NnmInstallDir/log/qa/qaspi0.log*

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

Importing Discovery Filters

To import discovery filter configurations from an XML file:

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

Import.
3. In the user prompt dialog, 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.

You can also import discovery filter using the following command line utility:

UNIX: *$NnmInstallDir/bin/nmsqadiscofilter.ovpl –import [filename]*

Windows: *%NnmInstallDir%\bin\nmsqadiscofilter.ovpl –import [filename]*

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

UNIX: *.$NnmInstallDir/log/qa/qaspi0.log*

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

Note: While you import a discovery filter from the previous version of NNM iSPI Performance for QA, the discovery filter name is automatically generated in this version of NNM iSPI Performance for QA.

HP Network Node Manager iSPI Performance for Quality Assurance Software Global Network Management Configuration

The Global Network Management (GNM) configuration of the NNM iSPI Performance for QA provides distributed deployment capabilities in a network environment. An implementation of NNM iSPI Performance for QA in a GNM environment is very similar to an implementation of NNMi in a GNM environment. For more information on the GNM feature, see the *Connecting Multiple NNMi management servers* topic in the *HP Network Node Manager i Software Online help*

Before you implement the GNM configuration for the NNM iSPI Performance for QA, you must have implemented the GNM configuration for NNMi. The global manager and regional managers configured in NNMi **must be the same** in NNM iSPI Performance for QA. For example, a regional manager (RM) in NNMi cannot be a global manager (GM) in NNM iSPI Performance for QA.

It is not mandatory to configure the NNM iSPI Performance for QA in a GNM environment if NNMi is configured in the GNM environment. In such instances, the NNM iSPI Performance for QA can be installed on the NNMi GM, and the GM discovers the nodes that are hosting the QA probes as local nodes.

You must make sure that in a GNM environment all the NNMi management servers have time synchronization.

For more information on the GNM scenarios in NNM iSPI Performance for QA, see the chapter *Deploying NNM iSPI Performance for QA in a Global Network Management Environment* in the *NNM iSPI Performance for Quality Assurance Software Deployment Reference* guide.

Related Topics

Launch the Global Network Management Configuration Form

Create a New Regional Manager

Edit an Existing Regional Manager

Delete an Existing Regional Manager

Launching the Global Network Management Configuration Form

Perform the following steps to launch the Global Network Management configuration form:

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

   You must have administrator privileges.
2. From the workspace navigation panel, select **Configuration** workspace.
3. Select **Quality Assurance Configuration Console**

   The console opens.
4. In the **Configuration** workspace, select **Global Network Management**

   The Global Network Management configuration form opens.

You can perform the following tasks using the Global Network Management Configuration form:

Icons Available in the Global Network Management Configuration Toolbar	Description
 New	Creates a new regional Manager
 Open	Opens the Modify Regional Manager Configuration form of the selected Regional Manager
 Delete	Deletes the selected regional manager
 Refresh	Refreshes and displays the last saved regional manager configurations
 Close	Closes the GNM form without saving the current configuration

You can view the following details if you have configured a regional manager

Field Name	Description
Name	The connection name for the regional NNMi management server.
Description	A description for the regional manager connection.
UUID	The Universally Unique Identifier of the regional manager.
Connection State	The Connection status can be either one of the following: • Not Established • Connected

Related Topics

Overview of Global Network Management Configuration

Create a New Regional Manager

Edit an Existing Regional Manager

Delete an Existing Regional Manager

Creating a New Regional Manager

To create a new regional manager:

1. Launch the Global Network Management Configuration form.
2. Click  **New** in the Global Network Management Configuration form.

   The Regional Manager Configuration form opens.
3. Enter values for the following:

Field Name	Description
Name	Type the connection name for the regional NNMi management server. Note: Make sure that the regional manager connection name is the same as the connection name specified for the NNMi
Description	This field is optional. Type a description for the regional manager.

4. Select any one of the following options:

Option	Description
 Close	Closes the Create New Regional Manager Configuration form without saving the information you entered.
 Save	Saves the regional manager configuration.

5. You can perform the following tasks when you click on the **Connections** tab.:

Icons Available in Connections Tab	Description
 New	Adds a new regional manager connection
 Open	Opens the Modify Regional Manager Connections form of the selected regional manager connection
 Delete	Deletes the details of the selected regional manager connection
 Refresh	Refreshes and displays the last saved regional manager connection

Related Topics

Overview of Global Network Management Configuration

Edit an Existing Regional Manager

Delete an Existing Regional Manager

Adding a Regional Manager Connection

1. Launch the Global Network Management Configuration form
2. Make sure that you enter the Name in the Create Regional Manager form.
3. Click  **New** in the **Connections** panel of the Create New Regional Manager Configuration form.

   The Add Regional Manager Connection form opens.
4. Enter values for the following:
   a. **Hostname**

      The Fully Qualified Domain Name (FQDN) of the NNMi management server which should be connected as the regional manager.

   b. **Use Encryption**

      If you select this option, NNM iSPI Performance for QA uses the Hypertext Transfer Protocol Secure (HTTPS) to connect to the regional NNMi management server.

      If you do not select this option NNM iSPI Performance for QA uses the Hypertext Transfer Protocol (HTTP) to connect to the regional NNMi management server.

      Note: If you selected HTTPS option in NNMi management server, you must select the Use Encryption option. However, if you selected the HTTP option in NNMi management server, you must clear the Use Encryption option.

   c. **HTTP(S) Port**

      If you selected the Use Encryption (previous field), you must enter the port number for the HTTPS protocol.

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

   d. **User Name**

      Type a valid user name of the regional NNMi management server.

   e. **User Password**

      Type the password of the User Name for the regional NNMi management server.

   f. **Ordering**

      A numeric value. NNM iSPI Performance for QA checks for configuration settings in the

order you define (lowest number first). NNM iSPI Performance for QA uses the first match found for each address. Provide a unique connection ordering number for each regional manager configuration.

Any duplicate Ordering numbers are checked in random order; for example that group of regional manager connections can be checked in any order during each discovery cycle.

5. Use any one of the following options:

Icons	Description
 Close	Closes the Add Regional Manager Connection form without saving the information you have entered
 Save	Saves the regional manager connection information
 Clear	Clears the regional manager connection information you have entered in the form

Related Topics

Overview of Global Network Management Configuration

Edit an Existing Regional Manager

Delete an Existing Regional Manager

Editing an Existing Regional Manager

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

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

To modify a regional manager:

1. Launch the Global Network Management Configuration form.
2. Select the regional manager to be modified in Global Network Management Configuration form.
3. Click  **Open** in the Global Network Management Configuration form.

   The Modify Regional Manager Configuration form opens.
4. You can modify the following information:

Field Name	Description
Name	Type the connection name for the regional NNMi management server. Note: Make sure that the regional manager connection name is the same as the connection name specified for the NNMi.

Field Name	Description
Description	This field is optional. Type a description for the regional manager connection.

5. Select any one of the following options:

Option	Description
Close	Closes the Add Regional Manager Connection form without saving the information you have entered.
Save	Saves the regional manager connection information.

6. Click on the **Connections** tab.
7. Do any one of the following tasks:

Icons Available in the Connections Panel	Description
New	Adds a new regional manager connection
Open	Opens the Modify Regional Manager Connections form of the selected regional manager connection
Delete	Deletes the details of the selected regional manager connection
Refresh	Refreshes the Regional Manager Connections panel and displays the last saved regional manager connection

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

To modify a regional manager connection:

1. Launch the Global Network Management Configuration form.
2. Select the regional manager to be modified in the Global Network Management Configuration form.
3. Click **Open** in the Global Network Management Configuration form.

   The Modify Regional Manager Configuration form opens.
4. Select the regional manager connection that needs to be modified in the Connections panel.

5. Click  **Open** in the Connections panel.

   The Modify Regional Manager Connection form opens.

6. You can modify the following information:

Field Name	Description
Use Encryption	If you select this option, NNM iSPI Performance for QA uses the Hypertext Transfer Protocol Secure (HTTPS) to connect to the regional NNMi management server. If you do not select this option, NNM iSPI Performance for QA uses the Hypertext Transfer Protocol (HTTP) to connect to the regional NNMi management server. Note: If you selected HTTPS option in NNMi management server, you must select the Use Encryption option. However, if you selected the HTTP option in NNMi management server, you must clear the Use Encryption option.
HTTP(S) Port	If you selected the Use Encryption (previous field), you must enter the port number of the HTTPS protocol. If you did not select the Use Encryption (previous field), you must enter the port number of the HTTP protocol.
User Name	Type a valid user name of the regional NNMi management server.
User Password	Type the password of the User Name for the regional NNMi management server.
Ordering	A numeric value. NNM iSPI Performance for QA checks for configuration settings in the order you define (lowest number first). NNM iSPI Performance for QAuses the first match found for each address. Provide a unique connection ordering number for each regional manager configuration. Any duplicate Ordering numbers are checked in random order; for example that group of regional manager connections can be checked in any order during each discovery cycle.

7. Select any one of the following options:

Icons	Description
 Close	Closes the Modify Regional Manager Connection form without saving the information you have entered
 Save	Saves the regional manager connection information

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

Related Topics

Overview of Global Network Management Configuration

Create a New Regional Manager

Delete an Existing Regional Manager

Deleting an Existing Regional Manager

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

To delete a regional manager configuration:

Note: If you delete a regional manager configuration, all the objects such as sites associated with the regional manager gets deleted.

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

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

To delete a regional manager connection:

Note: If you delete a regional manager configuration, all the objects such as sites associated with the regional manager gets deleted.

1. Launch the Global Network Management Configuration form.
2. Select the regional manager to be deleted in the Global Network Management Configuration form.
3. Click  **Open** in the Global Network Management Configuration form.

   The Modify Regional Manager Configuration form opens.
4. Select the regional manager connection in the Connections panel, and click  **Delete**
5. Click  **Refresh** in the Connections panel to view the changes.

HP Network Node Manager iSPI Performance for Quality Assurance Software Configure QA Probes

Probe configuration form enables you to do the following:

- Create a probe
  - Identify the type of test or probe to run on the node. For example, the QA probe service type, and VRF name etc.
  - Define the duration details to run the test or probe. For example, the frequency, the life time of the probe etc.
  - Optionally, define the payload details. For example, the the size of the packet, inter packet delay etc.
- Create a template for probe that can be reused and associated with any source and destination node
- Deploy the probe, or save the probe details to a file and deploy at a later point of time
- View the Real Time Line graph for the metrics of QA probes that are deployed successfully
- Reconfigure the probes if the deployment for the configured probes fail
- View the probe list and template list
- View the preconfigured probes and launch the real time line graph (if required)

Note: The NNM iSPI Performance for QA supports multitenant architecture. Multitenant architecture establishes a node to tenant association and determines the nodes that can be accessed by the user. However, you can configure the QA probes for a source node irrespective of whether you can access the destination node. A user with administrator privileges or Level 2 Operator access can configure probes.

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

Related Topics

Launch the Probe Configuration Form

Launching the Probe Configuration Form

Perform the following steps to launch the Probe Configuration form:

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

   You must have administrator privileges.

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

   To launch the Probe Configuration form from the Nodes Inventory

   a. Click **Inventory**. The Inventory expands.

   b. Click **Nodes**

   c. Select the required nodes in the Nodes inventory for which you need to configure the QA probes

   d. Go to step 3

   To launch the Probe Configuration form from the Network Overview

   a. Click **Topology Maps**. The Topology Maps expand.

   b. Click **Network Overview**

   c. Select the required nodes in the Network Overview for which you need to configure the QA probes

   d. Go to step 3

   To launch the Probe Configuration form from the Interfaces Inventory

   a. Click **Inventory**. The Inventory expands.

   b. Click **Interfaces**

   c. Select the required interfaces in the Interfaces inventory

   d. Go to step 3

   To launch the Probe Configuration form from the IP Addresses Inventory

   a. Click **Inventory**. The Inventory expands

   b. Click **IP Addresses**

   c. Select the required IP Addresses in the IP Addresses inventory

   d. Go to step 3

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

   The Probe Configuration form opens.

   The following icons are available in the Probe Configuration form:

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

Related Topics

Overview of Configure QA Probes

Probe Configuration Form: Probe Definition Tab

Probe Configuration Form: Probe List Tab

Probe Configuration Form: Template Definition Tab

Probe Configuration Form: Template List Tab

Probe Configuration Form: Probe Definition Tab

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

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

To create a new probe definition:

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

   Source Node Details

   Enter the following in the Source Node Details:

   Note: The asterisk * symbol against the field name indicates the field is mandatory.

Field Name	Description
Hostname *	Select the hostname of the source node for which you intend to configure the QA probes.
IP Address	Select the source IP address of the node.
Port Number	The source port from which you intend to configure QA probes. This field appears on selecting the Service in the Probe Definition form. This field is not applicable for ICMP echo service.
Write Community String	The write community string to use for authentication on the source node. If you leave this field blank, the SNMP Write Community String value is retrieved from NNMi.

Destination Node Details

Enter the following in in the Destination Node Details:

Note: The asterisk * symbol against the field name indicates the field is mandatory.

Field Name	Description
Hostname	Select the hostname of the destination node for which you intend to configure the QA probes.
IP Address *	Select the destination IP address of the node.
Port Number	The destination port number to which you intend to configure QA probes. This field is mandatory for UDP, UDP Echo, TCP Connect, and VOIP service

Note: You can click on **Enable Responder** and enter the Write Community String to enable the responder state.

3. Select the **Probe Definition** tab.
4. Enter the following Protocol Details :

   Note : You can expand or collapse the protocol details. The asterisk * symbol against the field name indicates the field is mandatory.

Field Name	Description
Probe Name *	The name of the QA probe.
Service *	Select the service type of the QA probe. The valid service types are: ▪ UDP Echo ▪ ICMP Echo

Field Name	Description
	▪ UDP ▪ TCP Connect ▪ VoIP Port Number field appears in the Destination Node details on selecting the Service. Port Number field does not appear if you selected ICMP echo service.
VRF Name	The name of the VRF.
ToS	The Type of Service specified in an IP packet header that indicates the service level required for the packet.

5. Enter the following Duration Details:

   Note : You can expand or collapse the probe duration details. The asterisk * symbol against the field name indicates the field is mandatory.

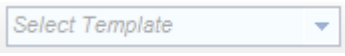
Field Name	Description
Frequency *	The frequency at which the specific QA probe test must be repeated. Click on this field to enter the hour, minute, and seconds.
Life Time	The life time of the QA Probe. The default value is `Forever`. To override this value, you can click on this field to enter the day, hour, and minute.
Time Out	Maximum time the source node will wait for a response from the destination node before stopping the probes to run on the node. Click on this field to enter the hour, minute, and seconds.

6. Enter the following Payload Details:

   Note: You can expand or collapse the Payload Details. The payload details appear based on the selected service. The asterisk * symbol against the field name indicates the field is mandatory.

Field Name	Description
Packet Size	The size of each packet.
Number of Packets	The number of packets sent. This field is applicable for UDP or VoIP service.
Inter Packet Delay (milliseconds)	The inter packet delay in milliseconds. This field is applicable for UDP or VoIP service.
Codec Type *	Select the codec type. This field is applicable for VoIP service.

7. You can also create a probe using a pre-defined probe template by following the step below:

   Select the template from the 

Select Template
8. To deploy a single probe follow the step below:

   Click  Deploy in the Probe Definition tab. The Deploy operation does the SNMP set operation on the selected source node.
9. To deploy probes in bulk, follow these steps:
   a. Click  Add to add the probes temporarily to the Probe List table below
   b. Click on the Probe List tab below to view the probes
   c. You can find a list of options on the left-side of the table.
   d. Select the probes, and click  Deploy
10. You can view the deploy status in the Deploy Status tab
11. Alternatively, you can save the probe configuration details to a file and deploy the probes at a later point of time. To save the probe configuration details to a file, you must click  **Save** in the main Probe Configuration form toolbar.

Related Topics

Configure QA Probes Overview

Launch the Probe Configuration Form

Probe Configuration Form: Probe List Tab

Deploy the QA Probes

Probe Configuration Form: Template Definition Tab

Probe Configuration Form: Deploy Status Tab

Probe Configuration Form: Preconfigured Probes Tab

Probe Configuration Form: Deploy Status Tab

You can use the **Deploy Status** tab to do the following tasks:

- View the probe deployment status
- Launch the real time graph
- Select the probes to be reconfigured. You can only reconfigure probes whose Deploy Status is Failure.

To view the probe deploy status:

1. Select the **Deploy Status** tab in the Probe Configuration form.
2. On the left pane, you can view the following details:

Field Name	Description
Total Count	The total number of probes that you attempted to deploy irrespective of the status.
In Progress Count	The number of probes that are being deployed.
Success Count	The number of probes that were successfully deployed.
Failed Count	The number of probes that did not get deployed successfully.

3. On the right pane, you can view the following details:

Field Name	Description
Operational Status	The deployment status of the probe. The valid statuses are: ▪ In-progress: Indicates the SNMP set operation is in-progress ▪ Success: Indicates the SNMP set operation is successful ▪ Failure: Indicates the SNMP set operation is a failure
Source Hostname	The hostname of the source node.
Probe Name	The name of the QA probe.
Owner	The owner of the QA probe.
Status Details	Displays a message on successful deployment of the probe, or indicates the reason for failure in the event of failure

You can view the percentage of QA probes deployed irrespective of the deployment status in the status bar.

4. Select any one of the following options:

Icons Available in the Deploy Status Tab	Description
 Edit	Allows to reconfigure the selected QA Probe details for which the deployment status is Failure
 Launch Real Time Graph	Launches the real time line graph in a new window for the selected probes and metric
 Refresh	Refreshes the details

Related Topics

Launch the Probe Configuration Form

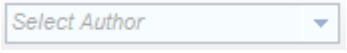
Probe Configuration Form: Template Definition Tab

You can use the **Template Definition** tab to do the following tasks:

- Define a QA probe template that can be reused and associated with any source and destination node
- Edit or view an existing template
- View the probe definition template based on the author name
- Copy the template definition

To define a new probe template:

1. Launch the Probe Configuration form.
2. Select the **Template Definition** tab.
3. Click  **New** in the toolbar below the **Template Definition** tab.
4. To view the existing templates based on the author

Field Name	Description
 Select Author	Select the author name to retrieve the template list based on the author. The system populates the drop-down list with the author names defined in NNMi. The template list appears in the table below only if any template exists for the selected author.

5. To enter a new template definition:

a. Select the following:

Field Name	Description
Select Author: Select Author	Select the author name to associate an author to the templates. The system populates the drop-down list with the author names defined in NNMi. On selecting the author, if the Read Only value is True, the user cannot edit the template. Note: The template list appears in the table below only if any template exists for the selected author.

b. Enter the following Protocol Details:

Note: You can expand or collapse the Protocol Details. The asterisk * symbol against the field name indicates the field is mandatory.

Field Name	Description
Template Name *	The name of the QA probe definition template.
Service *	Select the service type of the QA probe. The valid service types are: ○ UDP Echo ○ ICMP Echo ○ UDP ○ TCP Connect ○ VoIP
VRF Name	The name of the VRF.
ToS	The Type of Service specified in an IP packet header that indicates the service level required for the packet.

c. Enter the following Duration Details:

Note: You can expand or collapse the Duration Details. The asterisk * symbol against the field name indicates the field is mandatory

Field Name	Description
Frequency *	The frequency at which the QA probe test must be repeated. Click on this field to enter the hour, minute,

Field Name	Description
	and seconds.
Life Time	The life time of the QA Probe. The default value is `Forever`. To override this value, you can click on this field to enter the day, hour, and minute.
Time Out	Maximum time the source node will wait for a response from the destination node before stopping the probes to run on the node. Click on this field to enter the hour, minute, and seconds.

d. Enter the following Payload Details:

Note: You can expand or collapse the Payload Details. The payload details appear based on the selected service type. The asterisk * symbol against the field name indicates the field is mandatory

Field Name	Description
Packet Size	The size of each packet.
Number of Packets	The number of packets sent. This field is applicable for UDP or VoIP service.
Inter Packet Delay (milliseconds)	The inter packet delay in milliseconds.This field is applicable for UDP or VoIP service.
Codec Type *	Select the codec type from the drop-down list. This field is applicable for VoIP service.

e. Select any one of the following options:

Icons Available in the Template Definition Tab	Description
 New	Adds a new probe definition template
 Save	Saves the probe template definition
 Refresh	Refreshes the template definition details

f. Click on  **Save** in the Template Definition panel.

g. After you save the template definition details, the details appear in the table below.

6. Click on **Template List** tab to view the templates that were defined and saved in the Template Definition panel.

You can find a list of options on the left-side of the table.

7. Select any one of the following options (if required) listed below:

Icons Available in the Template List Tab	Description
 Open	Opens the selected template definition in the Template Definition form
 Copy	Copies the selected template that appears in the Template Definition form
 Delete	Deletes the selected template definition
 Select All	Selects or deselects all the templates in the template list

Related Topics

Configure QA Probes Overview

Launch the Probe Configuration Form

Probe Configuration Form: Probe Definition Tab

Probe Configuration Form: Template List Tab

Probe Configuration Form: Probe List Tab

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

- View the configured probe definition in a new window
- Delete the selected probe definition
- Open the selected probe
- Deploy the selected probes on the node
- Allows to select all the probes in the Probe List

To access the probe list:

1. Launch the Probe Configuration form

   You can view three tabs below the Probe Configuration form; Probe List, Template List, and Real Time Graph

2. Select the **Probe List** tab.

   You can view the following details:

Field Name	Description
Probe Name	The name of the QA probe.
Source IP Address	The source IP address of the node.
Destination IP Address	The destination IP address of the node.
Service	The service type of the QA probe can be any one of the following: ▪ UDP Echo ▪ ICMP Echo ▪ UDP ▪ TCP Connect ▪ VoIP
ToS	The Type of Service specified in an IP packet header that indicates the service level required for the packet.
VRF Name	The name of the VRF.
Frequency	The frequency at which the specific QA probe test must be repeated.
Source Port	The source port from which the QA probes are configured.
Destination Port	The destination port until which the QA probes are configured.
Life Time	The life time of the QA Probe.
Time Out	Maximum time the source node will wait for a response from the destination node before stopping the probes to run on the nod
Codec Type	The type of codec.
Source Hostname	The hostname of the source node for which the QA probes are configured.
Destination Hostname	The hostname of the destination node for which the QA probes are configured.

3. You can find a list of options on the left-side below the Probe Configuration form. Select any one of the following options (if required):

Icons Available in the Probe List Tab	Description
 Deploy	Deploys the selected configured probes on the selected node

 Open	Opens and allows to edit the selected probe definition
 Copy	Copies the selected probe that appears in the Probe Definition form
 Delete	Deletes the selected probe definition
 Select All	Selects or deselects all the probes in the probe list

Related Topics

Configure QA Probes Overview

Launch the Probe Configuration Form

Probe Configuration Form: Probe Definition Tab

Deploy the QA Probes

Probe Configuration Form: Template List Tab

Probe Configuration Form: Preconfigured Probes Tab

Probe Configuration Form: Template List Tab

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

- View the template definition in a new window
- Delete the selected template definition
- Allows to select all the templates in the Template List

To access the template list:

1. Launch the Probe Configuration form

   You can view two tabs below the Probe Configuration form; Probe List, and Template List
2. Select the **Template List** tab.

   You can view the following details:

Field Name	Description
Template Name	The name of the QA probe template.
Service	The service type of the QA probe can be any one of the following: ▪ UDP Echo ▪ ICMP Echo ▪ UDP

Field Name	Description
	▪ TCP Connect ▪ VoIP
VRF Name	The name of the VRF.
ToS	The Type of Service specified in an IP packet header that indicates the service level required for the packet.
Frequency	The frequency at which the specific QA probe test must be repeated.
Life Time	The life time of the QA Probe.
Time Out	Maximum time the source node will wait for a response from the destination node before stopping the probes to run on the nod
Codec Type	The type of codec.
Packet Size	The size of each packet.
Number of Packets	The number of packets sent.
Inter Packet Delay (milliseconds)	The inter packet delay in milliseconds.

3. You can find a list of options on the left-side below the Probe Configuration form. Select any one of the following options (if required):

Icons Available in the Template List Tab	Description
 Open	Opens and allows to edit the selected template in the Template Definition form
 Copy	Copies the selected template that appears in the Template Definition form
 Delete	Deletes the selected template definition
 Select All	Selects or deselects all the templates in the template list

Related Topics

Configure QA Probes Overview

Launch the Probe Configuration Form

Probe Configuration Form: Probe Definition Tab

Probe Configuration Form: Probe List Tab

Probe Configuration Form: Template Definition Tab

Probe Configuration Form: Deploy Status Tab

Probe Configuration Form: Preconfigured Probes Tab

You can use the **Preconfigured Probes** tab to view the list of configured probes discovered and monitored by NNM iSPI Performance for QA. Also, you can launch the real time line graph for the probes.

To view the preconfigured probes list:

1. Launch the Probe Configuration form
2. Select the **Preconfigured Probes** tab.

   You can view the following details:

Field Name	Description
Probe Status	The status that the QA probe returned. A QA probe may return any of the following statuses : ▪ Normal ▪ Warning ▪ Major ▪ Critical ▪ Unknown ▪ Disabled ▪ Not Polled ▪ No Status For more information on status, see the topic QA Probe Status
Probe Name	The name of the QA probe.
Owner	The owner of the QA probe.
Source Hostname	The hostname of the source node for which the QA probes are configured.
Destination IP Address	The destination IP address of the node.
Service	The service type of the QA probe. The valid service types are: ▪ UDP Echo ▪ ICMP Echo ▪ UDP

Field Name	Description
	▪ TCP Connect ▪ VoIP
VRF Name	The name of the VRF.
ToS	The Type of Service specified in an IP packet header that indicates the service level required for the packet.

3. To launch the Real Time Line Graph for the probes:
   a. Select the probes and select the metric from the drop-down list.
   b. Select  **Launch Real Time Graph**
   The Real Time Line Graph opens in a new window

   See the topic Real Time Line Graph for more information.

Related Topics

Configure QA Probes Overview

Launch the Probe Configuration Form

Probe Configuration Form: Probe Definition Tab

Deploy the QA Probes

Probe Configuration Form: Template List Tab

Probe Configuration Form: Template Definition Tab

Probe Configuration Form: Deploy Status Tab

HP Network Node Manager iSPI Performance for Quality Assurance Software Probe Maintenance

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

Launching the Probe Maintenance Form

Perform the following steps to launch the Probe Maintenance form:

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

   You must have administrator privileges.
2. Select **Actions** → **Quality Assurance** → **Probe Maintenance**

   The Probe Maintenance form opens.
3. Enter the following Node details:

Field Name	Description
Hostname	Select the hostname of the source node.
Write Community String	The write community string to use for authentication on the node.

4. Click on **Test SNMP** to check whether SNMP is working and validate the Write Community String of the node.

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

Related Topics

Probe Maintenance Form: Probe List Tab

Probe Maintenance Form: Enable Status Tab

Probe Maintenance Form: Disable Status Tab

Probe Maintenance Form: Delete Status Tab

Probe Maintenance Form: Probe List Tab

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

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

To view the probe list:

1. Launch the Probe Maintenance form.
2. Click on the **Probe List** tab.

   You can view the following details:

Field Name	Description
Probe Status	The status of the QA probe.
Probe Name	The name of the QA probe.
Owner	The QA probe owner name.
Source Hostname	The hostname of the source node.
Destination IP Address	The destination IP address of the node.
Service	The service type of the QA probe. The valid service types are: ▪ UDP Echo

Field Name	Description
	▪ ICMP Echo ▪ UDP ▪ TCP Connect ▪ VoIP
VRF Name	The name of the VRF.
ToS	The Type of Service specified in an IP packet header that indicates the service level required for the packet

3. Select any one of the following options:

Icons Available in the Probe List Tab	Description
 Select All	Selects all the probes
 Enable	Enables the selected probes and resumes the suspended operation
 Disable	Disables the selected probes and suspends the operation
 Delete	Deletes the selected probes from the device

Related Topics

Launch Probe Maintenance Form

Probe Maintenance Form: Disable Status Tab

Probe Maintenance Form: Enable Status Tab

Probe Maintenance Form: Delete Status Tab

Probe Maintenance Form: Enable Status Tab

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

- View the probes that are enabled
- View the percentage of QA probes enabled in the status bar

To access the probes that are enabled:

1. Launch the Probe Maintenance form.
2. Click on the **Enable Status** tab.

You can view the following details:

Field Name	Description
Operational Status	The operational status of the QA probe.
Source Hostname	The hostname of the source node.
Probe Name	The name of the QA probe.
Owner	The QA probe owner name.
Status Details	The status of the QA probe.

You can view a status bar which displays the percentage of QA probes that are enabled.

Related Topics

Launch Probe Maintenance Form

Probe Maintenance Form: Probe List Tab

Probe Maintenance Form: Disable Status Tab

Probe Maintenance Form: Delete Status Tab

Probe Maintenance Form: Disable Status Tab

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

- View the disable status
- View the percentage of QA probes disabled in the status bar

To access the probe list:

1. Launch the Probe Maintenance form.
2. Click on the **Disable Status** tab.

   You can view the following details:

Field Name	Description
Operational Status	The operational status of the QA probe.
Source Hostname	The hostname of the source node.
Probe Name	The name of the QA probe.
Owner	The QA probe owner name.
Status Details	The status of the QA probe.

You can view a status bar which displays the percentage of QA probes that are disabled.

Related Topics

Launch Probe Maintenance Form

Probe Maintenance Form: Probe List Tab

Probe Maintenance Form: Enable Status Tab

Probe Maintenance Form: Delete Status Tab

Probe Maintenance Form: Delete Status Tab

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

- View the deletion status
- View the percentage of QA probes deleted in the status bar

To access the probe list:

1. Launch the Probe Maintenance form.
2. Click on the **Delete Status** tab.

   You can view the following details:

Field Name	Description
Operational Status	The operational status of the node.
Source Hostname	The hostname of the source node.
Probe Name	The name of the QA probe.
Owner	The QA probe owner name.
Status Details	The status of the QA probe.

   You can view a status bar which displays the percentage of QA probes that are deleted.

Related Topics

Launch Probe Maintenance Form

Probe Maintenance Form: Probe List Tab

Probe Maintenance Form: Disable Status Tab

Probe Maintenance Form: Enable Status Tab

HP Network Node Manager iSPI Performance for Quality Assurance Software Probe Based Threshold Configuration

You can use the Configure Threshold form to perform the following tasks:

- Configure the threshold values for the metrics of selective QA probes
- Override the threshold values for the metrics of selective QA probes, which may or may not be associated to a site

You can configure thresholds for the following metrics assigned to the QA probes:

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

NNM iSPI Performance for QA performs the following actions if a threshold is breached:

- Sets the QA probe status to Major.
- Creates an incident for the violated threshold.
- Sends the threshold violation details to the Network Performance Server for generating reports
- Retains the threshold state as Nominal, or sets the threshold state to High or Low depending on the count based, and time based threshold configuration

You cannot configure thresholds for Remote QA Probes.

You can monitor the network performance and generate an incident based on the count based threshold configuration or time based threshold configuration.

Note: You can only configure either a count based or time based threshold configuration for a combination of a probe, service, and metric.

Threshold Configuration

Count Based Threshold Configuration

You can generate an incident based on the count or number of consecutive times a metric violates the threshold value. You can define this count in the Threshold Configuration form, and you can specify to trigger an incident when the threshold violation exceeds this count.

Time Based Threshold Configuration

Time based threshold configuration is useful when you intend to alert the user when the threshold breached state persists for more than a specific time period. This is derived by specifying X as the duration of time in minutes when the metric is in a threshold breached state within Y number of minutes specified in the sliding window. Based on your choice, you can trigger an incident if required.

Example for Time Based Threshold Configuration

Consider a scenario, where the polling interval is 5 minutes; High duration is 10 minutes; and High Duration Window is 60 minutes. In this scenario, an incident is generated whenever the High Duration exceeds 10 minutes within the 60 minute duration. NNM iSPI Performance for QA uses a sliding window wherein each time the High Duration (10 minutes) is reached, NNM iSPI Performance for QA drops the oldest polled value (first 5 minutes) and adds the most recent (between 60 to 65 minutes). This procedure continues and enables you to determine time based threshold violation.

You can make utmost use of the Time based threshold violation by ensuring that the duration specified in the sliding window is greater than or equal to the polling interval.

Baseline Settings Configuration

Baseline Deviation Settings Configuration

Apart from the time based and count based threshold configuration, you can also do a baseline monitoring based on the baseline deviation setting configuration in NNM iSPI Performance for QA. You can do a baseline deviation setting configuration for the selected probe, service, and metric. An incident is generated and the baseline state transitions to Abnormal Range only if it meets all the criteria listed below:

- Exceeds the count or the number of standard deviation that is above the average value for the metric, or exceeds the count or the number of standard deviation that is below the average value for the metric.This count is specified in the Upper Baseline Limit Deviations or the Lower Baseline Limit Deviations in the baseline deviation settings configuration
- Exceeds the duration for which the upper or lower baseline deviation persists in the specified sliding window duration

Related Topics

Launch the Configure Threshold Form

Add a New Threshold for QA Probes

Edit an Existing Threshold for QA Probes

Add New Baseline Settings for QA Probes

Edit an Existing Baseline Settings for QA Probes

Delete an Existing Threshold of QA Probes

Delete All Existing Thresholds of QA Probes

Delete a Baseline Setting of the QA Probe

Delete all Baseline Setting of the QA Probe

Launching the Configure Threshold Form

To launch the Configure threshold form:

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

   You must have administrator privileges.

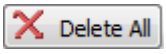
2. From the workspace navigation panel, select **Quality Assurance**

   The Quality Assurance tab expands.

3. Select any one of the following inventory views:
   - QA Probes
   - Critical Probes
   - Threshold Exception Probes
   - Baseline Exception Probes
4. Select the QA probes for which you need to configure the threshold value
   Note: You can select a maximum of 10 QA probes at one point of time

5. Click **Actions** → **Quality Assurance** → **Configure Threshold**
   - If you are configuring a new threshold value for the selected QA probes, the Add Threshold Configuration form opens.
   - If a threshold value already exists for the selected QA probes, the Edit Threshold Configuration form opens
   - If you selected Remote QA Probes, a message appears to indicate that you cannot configure thresholds for the remote QA probes. It also shows the list of remote QA probes selected.

Icons Available in the Threshold Configuration Toolbar	Description
 Close	Closes the Threshold Configuration form without saving the current configuration
 Save and Close	Saves the current configuration and closes the Threshold Configuration form
Icons Available in the Threshold Settings Tab	**Description**
 New	Adds a new threshold for the QA probes
 Edit	Edits/Overrides an existing threshold for the QA probes
 Delete	Deletes an existing threshold of the QA probes
 Refresh	Retrieves the last saved threshold configuration from the database and displays the data
 Delete All	Deletes all the existing thresholds of the QA probes

Icons Available in the Baseline Settings Tab	Description
 New	Adds a baseline settings for the QA probes
 Edit	Edits/Overrides an existing baseline setting for the QA probes
 Delete	Deletes an existing baseline setting of the QA probes
 Refresh	Retrieves the last saved baseline settings configuration from the database and displays the data
 Delete All	Deletes all the existing baseline settings of the QA probes

Related Topics

Overview of Configure Threshold for QA Probes

Add a New Threshold for QA Probes

Edit an Existing Threshold for QA Probes

Add New Baseline Settings for QA Probes

Edit an Existing Baseline Settings for QA Probes

Delete an Existing Threshold of QA Probes

Delete All Existing Thresholds of QA Probes

Delete a Baseline Setting of the QA Probe

Delete all Baseline Setting of the QA Probe

Adding New Threshold Settings Using the Threshold Configuration Form

To add a new threshold:

1. Make sure that you selected the Source Site, and Service in the Add Threshold Configuration form if you are launching the form from Site Wide threshold configuration. You can ignore this step if you are launching this form from Probe based threshold configuration.
2. Click  **New** in the **Threshold Settings** tab.

   The Add Threshold Settings form opens.
3. Specify the following to configure the threshold settings:

Field Name	Description
Type	Select the type of threshold violation. The valid types are Count Based and Time Based.
Metric	Select the metric for which you are configuring the threshold. The metrics are populated based on the service.

4. After you select the metric to configure the threshold, the list of fields relevant to the selected metric appear. You can specify the following values to configure the new threshold:

Field Name	Description
High Value	Enter the threshold value. This value indicates the maximum value above which the metric will be considered to have violated the Nominal range. For Packet Loss metric, enter the High Value in percentage.
High Value Rearm	Enter the high rearm value for the threshold. For Packet Loss metric, enter the High Value Rearm in percentage. The High Rearm Value is used to indicate the end of the high threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value. The high value rearm must always be lower than the high value. **Example** For the Round Trip Time (RTT) you must generate an incident when the RTT is 150 and clear the incident when the RTT value comes down to 100. Set the following values for the threshold: ▪ High Value: `150` ▪ High Value Rearm: `100` This value enables you to be aware when a network performance problem starts to improve.
Low Value	Enter the low threshold value. This value indicates the maximum value below which the metric will be considered to have violated the Nominal range.
Low Value Rearm	Enter the low rearm value for the threshold. For Packet Loss metric, enter the Low Rearm Value in percentage. The Low Rearm Value is used to indicate the end of the low threshold state and NNM iSPI Performance for QA clears the incident once it reaches above this value. The low value rearm must be greater than the low value. **Example** For the Mean Opinion Score (MOS) you must generate an incident when the MOS score is 3 and clear the incident when the score is improved to 4.5. Set the following values for the threshold:

Field Name	Description
	▪ Low Value: 3 ▪ Low Value Rearm: 4.5 This value enables you to be aware when a network performance problem starts to improve.

The following field appears, if you selected the Type as Count Based:

Field Name	Description
Trigger Count	Specify after how many consecutive threshold violations NNM iSPI Performance for QA must alert the operator by transitioning the threshold state to High or Low accordingly.

The following fields appear if you selected the Type as Time Based:

Field Name	Description
High Duration	The minimum duration for which the value must persist in a high value range for the threshold state to change to High and generate an incident (if specified). The polling interval must be less than or equal to the high duration value.
High Duration Window	The duration of the window within which the high duration criteria must be met. This value must be greater than 0 (zero), and this value can be the same as High Duration value. NNM iSPI Performance for QA uses a sliding window wherein each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polled value and adds the most recent.

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

Low Duration	The minimum duration for which the value must persist in a low value range for the threshold state to change to Low and generate an incident (if specified). The polling interval must be less than or equal to this low duration value.
Low Duration Window	The duration of the window within which the low duration criteria must be met. This value must be greater than 0 (zero), and this value can be the same as Low Duration value. NNM iSPI Performance for QA uses a sliding window wherein each time the Low Window Duration is reached, NNM iSPI Performance for QA drops the oldest polled value and adds the most recent.

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

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

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

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

7. Click **Refresh** to view the changes.
8. Click **Save** or **Save and Close** in the Threshold Configuration form.

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

NNM iSPI Performance for QA applies the following rules while creating thresholds for a **site** using this form:

- You can create thresholds only for the existing sites.
- You must select a source site and service for the new threshold.
- You could select the destination site for the new threshold
- If you do not specify a destination site for the threshold, the threshold is applied to all the destination sites of the source sites.
- You cannot configure thresholds for remote sites.

Note: For a Time Based Threshold configuration on probes, if the polling interval is greater than the High Duration or Low Duration value, the threshold cannot be configured for those QA probes. A list of these QA Probes, the UUID, and other details can be viewed in the log file, which is available in the following directory:

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

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

Related Topics

Overview of Threshold Configuration for Sites

Overview of Threshold Configuration for Probes

Editing an Existing Threshold Setting Using the Threshold Configuration Form

To edit an existing threshold setting:

1. Make sure that you selected the Source Site, and Service in the Edit Threshold Configuration form if you are launching the form from Site Wide threshold configuration. You can ignore this step if you are launching this form from Probe based threshold configuration in the NNMi console or the Probe Specific Thresholds Form in the Quality Assurance Configuration console.
2. Click on the **Threshold Settings** tab.
3. Select the threshold setting to be modified, and click  **Edit**.

   The Edit Threshold Settings form opens.

   You can view the threshold setting that was configured earlier.

   Note: For probe based threshold configuration, you can view the threshold that was configured for the Remote QA probes, but you **cannot** configure thresholds for Remote QA Probes.

   You cannot modify the following details:

Field Name	Description
Type	The type of threshold violation can be Count Based or Time Based.
Metric	The name of the metric.

4. You can modify the following information:

Field Name	Description
High Value	Enter the threshold value. This value indicates the maximum value above which the metric will be considered to have violated the Nominal range. For Packet Loss metric, enter the High Value in percentage.
High Value Rearm	Enter the high rearm value for the threshold. For Packet Loss metric, enter the High Value Rearm in percentage. The High Rearm Value is used to indicate the end of the high threshold state and NNM iSPI Performance for QA clears the incident once it reaches below this value. The high value rearm must always be lower than the high value. **Example** For the Round Trip Time (RTT) you must generate an incident when

Field Name	Description
	the RTT is 150 and clear the incident when the RTT value comes down to 100. Set the following values for the threshold: ▪ High Value: `150` ▪ High Value Rearm: `100` This value enables you to be aware when a network performance problem starts to improve.
Low Value	Enter the low threshold value. This value indicates the maximum value below which the metric will be considered to have violated the Nominal range.
Low Value Rearm	Enter the low rearm value for the threshold. For Packet Loss metric, enter the Low Rearm Value in percentage. The Low Rearm Value is used to indicate the end of the low threshold state and NNM iSPI Performance for QA clears the incident once it reaches above this value. The low value rearm must be greater than the low value. **Example** For the Mean Opinion Score (MOS) you must generate an incident when the MOS score is 3 and clear the incident when the score is improved to 4.5. Set the following values for the threshold: ▪ Low Value: `3` ▪ Low Value Rearm: `4.5` This value enables you to be aware when a network performance problem starts to improve.

The following fields appear, if the Type is Count Based, and you can modify the information if required

Field Name	Description
Trigger Count	Specify after how many consecutive threshold violations NNM iSPI Performance for QA must alert the operator by transitioning the threshold state to High or Low accordingly.

The following fields appear if the Type is Time Based, and you can modify the information if required:

Field Name	Description
High Duration	The minimum duration for which the value must persist in a high value range for the threshold state to change to High and generate an incident (if specified) The polling interval must be less than or equal to the high duration value.
High Duration Window	The duration of the window within which the high duration criteria must be met. This value must be greater than 0 (zero), and this value can be the same as High Duration value. NNM iSPI Performance for QA uses a sliding window wherein each time the High Window Duration is reached, NNM iSPI Performance for QA drops the oldest polled value and adds the most recent.

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

Note: You can modify the information if required.

Low Duration	The minimum duration for which the value must persist in a low value range for the threshold state to change to Low and generate an incident (if specified). The polling interval must be less than or equal to this low duration value.
Low Duration Window	The duration of the window within which the low duration criteria must be met. This value must be greater than 0 (zero), and this value can be the same as Low Duration value. NNM iSPI Performance for QA uses a sliding window wherein each time the Low Window Duration is reached, NNM iSPI Performance for QA drops the oldest polled value and adds the most recent.

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

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

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

Icons	Description
 Close	Closes the Add Threshold Configuration form without saving the threshold

Icons	Description
	information you have entered
Save and Close	Saves the threshold information and closes the Threshold Configuration form
Clear	Clears the threshold information you have entered in the form

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

   The Threshold Configurations form closes.
9. Click **Save** or **Save and Close** in the Threshold Configuration form.

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

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

- You can define thresholds only for the existing sites.
- Any modification in the threshold directly updates the state poller.

Note: For a Time Based Threshold configuration on probes, if the polling interval is greater than the High Duration or Low Duration value, the threshold cannot be configured for those QA probes. A list of these QA Probes, the UUID, and other details can be viewed in the log file, which is available in the following directory:

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

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

Related Topics

Overview of Threshold Configuration for Sites

Overview of Threshold Configuration for Probes

Baseline Monitoring

Apart from the time based and count based threshold configuration, you can also do a baseline monitoring. Baseline monitoring is dynamic and updates the baseline state by comparing the extent of deviation from the average real-time data of the metric with the previous average values in a similar situation. For example, in a site during the peak hours or on week days, the RTT value is expected to exceed the high value frequently. In such a scenario, an incident need not be generated in the NNMi console. So, HP NNM iSPI Performance for Metrics Software enables you to compare the current threshold values during the peak hours with the previous set of values during the same peak hours. Based on the extent of deviation, you can configure to generate an incident in the NNMi console.

Baseline State

Baseline Monitoring sets a new state referred to as Baseline state for the QA probes. The valid baseline states for the QA probes are listed below:

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

Incidents

The following incidents are generated whenever there is a deviation from the configured normal range of deviation for the metric:

- RoundTripTimeAbnormal
- TwoWayPacketLossAbnormal
- TwoWayJitterAbnormal
- MeanOpinionScoreAbnormal

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

Adding New Baseline Settings Using the Threshold Configuration Form

To add a new baseline setting configuration:

2. 1. Make sure that you selected the Source Site, and Service in the Add Threshold Configuration form if you are launching the form from Site Wide threshold configuration. You can ignore this step if you are launching this form from Probe based threshold configuration.
   2. Click **New** in the **Baseline Settings** tab.
   The Add Baseline Settings form opens.
   3. Specify the following to configure the baseline deviation settings:

      Note: You can expand or collapse the baseline deviation settings.

Field Name	Description
Metric	Select the metric for which you require to configure baseline deviation settings. The valid metrics for baseline deviation

Field Name	Description
	setting configuration are as below: ▪ RTT (ms) ▪ RTT (microS) ▪ Two Way Jitter (microS) ▪ Two Way Packet Loss (%) ▪ MOS

4. After you select the metric, the list of fields relevant to the selected metric appear. You can specify the following values to configure the baseline deviation settings:

Field Name	Description
Upper Baseline Limit Enabled	If you enable this option, NNM iSPI Performance for QA uses the Upper Baseline Limit Deviations-Above Average field value to determine the number of times there is a standard deviation above the average value. If you disable this option NNM iSPI Performance for QA does not consider the Upper Baseline Limit Deviations-Above Average field value. This field is not relevant and does not appear for MOS metric.
Upper Baseline Limit Deviations - Above Average	The number or count of standard deviation above the average values for NNM iSPI Performance for QA to determine the upper baseline limit. This field is not relevant and does not appear for MOS metric.
Lower Baseline Limit Enabled	If you enable this option, NNM iSPI Performance for QA uses the Lower Baseline Limit Deviations-Below Average field value to determine the number of times there is a standard deviation below the average value. If you disable this option NNM iSPI Performance for QA does not consider the Lower Baseline Limit Deviations - Below Average field value. This field appears only for MOS metric.
Lower Baseline Limit Deviations - Below Average	The number or count of standard deviation below the average values for NNM iSPI Performance for QA to determine the lower baseline limit. This field appears only for MOS metric.
Duration	The minimum time for which the standard deviation must persist to deviate from the configured Baseline Range before the baseline state transitions to Abnormal Range and generates an incident.

Field Name	Description
	The Polling Interval should be less than or equal to the Duration.
Window Duration	The window duration within which the Upper Baseline Limit or Lower Baseline Limit Deviation criteria must be met. The value must be greater than 0 (zero) and can be the same as the Duration value. NNM iSPI Performance for QA uses a sliding window, meaning that each time the Duration is reached, NNM iSPI Performance for QA drops the oldest polling cycle and adds the most recent.

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

Icons	Description
 Close	Closes the Add Baseline Settings form without saving the baseline setting information you have entered.
 Save and Close	Saves the baseline setting information and closes the Add Baseline Settings form

6. Click  **Save and Close** in the Add Baseline Settings form to save the baseline setting information.

7. Click  **Save** or  **Save and Close** in the Threshold Configuration form.

   Caution: The new baseline settings configuration is not saved unless you click  **Save** or  **Save and Close** in the Threshold Configuration form.

   NNM iSPI Performance for QA applies the following rules while configuring baseline deviation settings for a **site** using this form:

   - You can configure baseline settings only for the QA probes of the existing sites.
   - You must select a source site, service, and metric to configure the baseline settings.
   - Optionally, you can select the destination site
   - If you do not specify a destination site for the baseline setting, the configuration is applied to all the QA probes of the destination sites from the source sites.
   - You cannot configure baseline settings for remote sites.

Related Topics

Overview of Threshold Configuration for Sites

Overview of Threshold Configuration for QA Probes

Editing Baseline Settings Using the Threshold Configuration Form

To edit a baseline setting configuration:

1. Make sure that you selected the Source Site, and Service in the Edit Threshold Configuration form if you are launching the form from Site Wide threshold configuration. You can ignore this step if you are launching this form from Probe based threshold configuration.
2. Select the baseline settings, and click  **Edit** in the **Baseline Settings** panel.

   The Edit Baseline Settings form opens.
3. To edit the baseline deviations settings in the **Baseline Deviations Settings** panel:
   a. You can view the following details:

Field Name	Description
Metric	The metric for which you require to edit the baseline deviations settings configuration.

   b. You can edit the following baseline deviation settings configuration:

   Note: The following fields appear depending on the metric:

Field Name	Description
Upper Baseline Limit Enabled	If you enable this option, NNM iSPI Performance for QA uses the Upper Baseline Limit Deviations-Above Average field value to determine the number of times there is a standard deviation above the average value. If you disable this option NNM iSPI Performance for QA does not consider the Upper Baseline Limit Deviations-Above Average field value. This field is not relevant and does not appear for MOS metric.
Upper Baseline Limit Deviations - Above Average	The number or count of standard deviation above the average values for NNM iSPI Performance for QA to determine the upper baseline limit. This field is not relevant and does not appear for MOS metric.
Lower Baseline Limit Enabled	If you enable this option, NNM iSPI Performance for QA uses the Lower Baseline Limit Deviations-Below Average field value to determine the number of times there is a standard deviation below the average value.

Field Name	Description
	If you disable this option NNM iSPI Performance for QA does not consider the Lower Baseline Limit Deviations - Below Average field value. This field appears only for MOS metric.
Lower Baseline Limit Deviations - Below Average	The number or count of standard deviation below the average values for NNM iSPI Performance for QA to determine the lower baseline limit. This field appears only for MOS metric.
Duration	The minimum time for which the standard deviation must persist to deviate from the configured Baseline Range before the baseline state transitions to Abnormal Range and generates an incident. The Polling Interval should be less than or equal to the Duration.
Window Duration	The window duration within which the Upper Baseline Limit or Lower Baseline Limit Deviation criteria must be met. The value must be greater than 0 (zero) and can be the same as the Duration value. NNM iSPI Performance for QA uses a sliding window, meaning that each time the Duration is reached, NNM iSPI Performance for QA drops the oldest polling cycle and adds the most recent.

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

Icons	Description
 Close	Closes the Edit Baseline Settings form without saving the baseline setting information you have entered.
 Save and Close	Saves the baseline setting information and closes the Edit Baseline Settings form

5. Click  **Save and Close** in the Edit Baseline Settings form to save the baseline setting information.

6. Click  **Save** or  **Save and Close** in the Site Wide Threshold Configuration form.

Caution: The new baseline settings configuration is not be saved unless you click  **Save** or  **Save and Close** in the Threshold Configuration form.

NNM iSPI Performance for QA applies the following rules while configuring baseline deviation settings for a **site** using this form:

- You can configure baseline settings only for the QA probes of the existing sites.
- You must select a source site and service to configure the baseline settings.
- Optionally, you could select the destination site
- If you do not specify a destination site for the baseline setting, the configuration is applied to all the QA probes of the destination sites from the source sites.
- You cannot configure baseline settings for remote sites.

Related Topics

Overview of Threshold Configuration for Sites

Overview of Threshold Configuration for QA Probes

Deleting an Existing Threshold of QA Probes Using the Edit Threshold Configuration Form

To delete an existing threshold of QA probes:

1. Launch the Configure Threshold form.
2. Select a threshold in the **Threshold Settings** panel and click **Delete**.
3. Click **Refresh** in the Threshold Settings panel to view the changes.

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

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

Example 1

Consider the following scenario:

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

QA Probe Status : Major

Threshold State: High

Note: The threshold state is high for RTT and Packet Loss

Conclusion: RttThresholdStateHigh, TwoWayPktLossThresholdStateHigh, RTTAbnormal

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

QA Probe Status : Major

Threshold State: Threshold Not Set

Note: The threshold state is set to Threshold Not Set for RTT and Packet Loss. If the QA probe is associated to a site the Threshold State is updated based on the threshold configured for the site.

Conclusion: RTTAbnormal

Note: The QA Probe Status is still set to Major as the Baseline State is in the Abnormal Range.

Example 2

Consider the following scenario:

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

QA Probe Status : Major

Threshold State: High

Conclusion: TestUp When both Administrative and Operational states are up., RttThresholdStateHigh,TwoWayPktLossThresholdStateHigh

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

QA Probe Status : Normal

Threshold State: Threshold Not Set

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

Conclusion: TestUp When both Administrative and Operational states are up.

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

To delete all the existing thresholds of QA probes:

1. Launch the Configure Threshold form.
2. Click Delete All **Delete All**.
3. Click **Refresh** in the Threshold Settings panel to view the changes.

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

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

Example 1

Consider the following scenario:

Before Deleting all the Thresholds Configured for the QA Probe

QA Probe Status : Major

Threshold State: High

Note: The threshold state is high for RTT and Packet Loss

Conclusion: RttThresholdStateHigh, TwoWayPktLossThresholdStateHigh, RTTAbnormal

After Deleting all the Thresholds Configured for the QA Probe:

QA Probe Status : Major

Threshold State: Threshold Not Set

Note: The threshold state is set to Threshold Not Set for RTT and Packet Loss. If the QA probe is associated to a site, the Threshold State is updated based on the threshold configured for the site.

Conclusion: RTTAbnormal

Note: The QA Probe Status is still set to Major as the Baseline State is in the Abnormal Range.

Example 2

Consider the following scenario:

Before Deleting all the Thresholds Configured for the QA Probe

QA Probe Status : Major

Threshold State: High

Conclusion: TestUp When both Administrative and Operational states are up., RttThresholdStateHigh,TwoWayPktLossThresholdStateHigh

After Deleting all the Thresholds Configured for the QA Probe:

QA Probe Status : Normal

Threshold State: Threshold Not Set

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

Conclusion: TestUp When both Administrative and Operational states are up.

HP Network Node Manager iSPI Performance for Quality Assurance Software Discovery Filter Configuration

Note: The error log files are available in the following directory:

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

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

QA probe filtering is not enabled. Please enable it.

Occurs if you have not enabled the Enable Discovery Filters option in the Discovery Filter Configuration form.

Reason and Resolution

Select the Enable Discovery Filters option in the Discovery Filter Configuration form.

Failed to import the discovery filter configuration. Please check the log files.

Occurs if the import file does not exist in the path you entered.

Reason and Resolution

NNM iSPI Performance for QA imports the discovery filter configuration from an XML file. If the file path is not correct, NNM iSPI Performance for QA fails to import the configuration information.

Check any of the following log files:

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

Windows: *%NnmInstallDir%\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*

Invalid QA probe owner name pattern.

Occurs if the Exclude Probe Owner Name Patterns field in the Discovery Filter Configuration form contains any illegal character.

Reason and Resolution

Avoid using '(Single quotation) as a QA probe owner name. NNM iSPI Performance for QA does not accept this character in a QA probe owner name.

Invalid Filter Name

Occurs when you try to save the discovery filter configuration details with an invalid filter name

Reason and Resolution

Avoid using '(Single quotation) in the filter name. NNM iSPI Performance for QA does not accept this character in a filter name.

Service Already Chosen

Occurs when you selected a service from the Service drop down list in the Discovery Filter Configuration form

Reason and Resolution

Do not select the same service again and add to the list.

HP Network Node Manager iSPI Performance for Quality Assurance Software Site Configuration

Note: The error log files are available in the following directory:

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

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

Failed to create the site. Please check the log files.

May occur for various reasons. Some of the reasons are as follows:

- If a site with the same name already exists. NNM iSPI Performance for QA recognizes a site by its name. Site names must be unique.
- If the IP address range is not valid.
- If the node group you specified does not exist in the NNMi database.

Reason and Resolution

Check any of the following log files:

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

Windows: *%NnmInstallDir%\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.

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: *%NnmInstallDir%\log\qa\qaspi0.log*

Site name already exists, cannot add new site

Occurs when you try to save site configurations with a site name that already exists

Reason and Resolution

You must enter a unique name for the site in the Site Configuration form. Site names are unique for a manager or NNMi management server.

Invalid Node Group Name cannot add new site

Occurs when you enter an invalid Node Group Name in the Site Configuration form.

Reason and Resolution

Enter a valid node group name

Update failed, invalid node group specified

Occurs when you try to save the site details in the Edit Site Configuration form, and you specified an invalid node group

Reason and Resolution

You must enter a valid node group configured in NNMi

Unable to write/retrieve data from the server

Occurs due to any exceptions raised while retrieving data from the server

Reason and Resolution

Check any of the following log files:

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

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

HP Network Node Manager iSPI Performance for Quality Assurance Software Threshold Configuration

Note: The error log files are available in the following directory:

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

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

Selected different service type. Deleting all settings.

Occurs when you select a different service type, while creating a new threshold or editing an existing threshold.

Reason and Resolution

NNM iSPI Performance for QA creates threshold for a metric based on the service type you have selected. Metrics available for different service types are different. For example, if you select TCP Connect service type, you can set thresholds for only the Round Trip Time (RTT) metric.

Changing the service type for a threshold may need you to update the threshold values for all the metrics. NNM iSPI Performance for QA deletes all the metric threshold values you have set previously, if you select a different service type.

Configuration already has the possible settings. Cannot add more.

Occurs if you click  **New** in the Threshold Settings panel of the Add Threshold Configuration form after creating a threshold.

Reason and Resolution

While creating a threshold, you performed the following steps:

1. Selected the following values in the Threshold Configuration panel in the Add Threshold Configuration form:
   a. Source Site
   b. Destination Site
   c. Service Type
2. Clicked  **New** in the Add Threshold Settings panel.
3. In the Threshold Configuration form, you selected the metric, high value, low value, high value rearm, low value rearm, etc.
4. Selected  **Save and Close** in the Threshold Configuration form. The threshold is added in the Threshold Settings panel of the Add Threshold Configuration form.
5. Clicked  **New** in the Threshold Settings panel.
6. The system displays an error message saying "The threshold already has the possible settings. Cannot add more."

You cannot add more than one set of threshold settings for a threshold configuration.

Failed to import the threshold configuration. Please check the log files.

Occurs under any of the following circumstances:

- If the import file does not exist in the path you entered.
- If a threshold is already defined and displayed in the Site Wide Threshold Settings panel.

Reason and Resolution

NNM iSPI Performance for QA imports the threshold configuration from an XML file. If the file path is not correct, NNM iSPI Performance for QA fails to import the configuration information.

Also the import utility does not import the threshold configuration if the configuration is unchanged since the last import

Check any of the following log files:

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

Windows: *%NnmInstallDir%\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 threshold to a destination site.

Check any of the following log files:

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

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

Duration of poll window cannot be greater than duration of sliding window

Occurs when the duration of the sliding window or Window Duration is greater than the polling window.

Reason and Resolution

The polling window duration must be lesser than the sliding window duration

Duration should be between 0 and 1400 minutes(1day)

Occurs when the low duration or high duration value (in minutes) for a time based threshold is not within the range

Reason and Resolution

The Low Duration or the High Duration value(in minutes) for a time based threshold must be within the range 0 to 1400 minutes (equivalent to 1 day).

Duration should be between 0 and 60 seconds

Occurs when the low duration or high duration value (in seconds) is not within the range

Reason and Resolution

The Low Duration or the High Duration value(in seconds) must be within the range 0 to 60 seconds

Import failed, file not found

Occurs when you import a threshold configuration

Reason and Resolution

You must import by specifying the absolute path of the file, and you must check the XML filename as well. The file to be imported must be available on the NNMi management server.

HP Network Node Manager iSPI Performance for Quality Assurance Software Global Network Management Configuration

Note: The error log files are available in the following directory:

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

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

Regional manager name has to be specified before creating new connection

Occurs when you try to add a new connection without entering the Regional Manager Name in the Regional Manager Configuration form.

Reason and Resolution

Before entering the regional manager connection details, you must enter the Regional Manager name in the Regional Manager Configuration form of NNM iSPI Performance for QA.

No connections configured

Occurs when you try to save the Add Regional Manager Connections form without entering the details

Reason and Resolution

You must enter the details in the Add Regional Manager Connections form before saving the details

An error occurred while modifying regional manager connection

Occurs when you try to save the modified regional manager connection details in the Regional Manager Configuration form

Reason and Resolution

Check any of the following log files:

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

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

Invalid parameters for connection

Occurs when you try to save the regional manager connection details in the Regional Manager Configuration form

Reason and Resolution

Check the parameters entered in the Regional Manager connection form

Check any of the following log files:

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

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

Connection parameters cannot be empty

Occurs when you try to save the regional manager connection details without entering the mandatory fields in the Add Regional Manager Connection form

Reason and Resolution

Enter the mandatory fields in the Add Regional Manager Connection form

Invalid Regional manager connection configuration information provided. NNMi cannot connect to: {1} {0}

Occurs when you trt to save the Regional Manager Configuration form

Reason and Resolution

Check if you have entered the correct hostname, username, and password

Duplicate Ordering

Occurs when you enter an ordering number in the Add Regional Manager Connection form that is assigned to some other regional manager connection

Reason and Resolution

You must enter an ordering number that is not assigned to some other regional manager connection

Failed to add connection {0} for regional manager {1}

Occurs when you try to save the regional manager connection details in the Add Regional Manager Connection form.

Reason and Resolution

Check any of the following log files:

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

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

Valid Port Number ranges from 0 to 65535

Occurs when you try to save the regional manager connection details with invalid HTTP or HTTPS port number range

Reason and Resolution

You must enter the HTTP or HTTPS port number of NNM iSPI Performance for QA running on the Regional Manager . The valid range is between 0 to 65535, but you can use the port number range between 1024 to 65535 preferably.

Use Case for HP Network Node Manager iSPI Performance for Quality Assurance Software Threshold Configuration

Module	HP Network Node Manager iSPI Performance for Quality Assurance Software Threshold Configuration
Use Case Name	Configuring Site Based Thresholds for Two Way Jitter in VoIP Network
Use Case Author	HP Software

Summary

This use case provides a step by step process overview on creating threshold settings for two way jitter on a VoIP network.

Application

VoIP

Overview

To ensure end-to-end bandwidth with minimum jitter. If the two way jitter in the traffic flow is higher than 75, an incident will be generated.

Actors

- Network Administrator
- Capacity Planner
- Business Managers
- Network Designers
- Architects involved in deploying the network

Pre Condition

At least one site must be created before adding the threshold settings.

In this use case we have two sites, `SiteA` and `SiteB`. We need to monitor the two way jitter between these two sites.

Configure Threshold

Assumptions

- User has administrative privileges to NNMi.
- User is using VoIP services to link between SiteA and SiteB.
- User wants to monitor the two way jitter(µsecs) between Site A and SiteB.
- Both SiteA and SiteB are created in the NNMi Performance SPI for Quality Assurance Site Configuration form.

Initialization

1. Log on to NNMi console using a username and password with administrator privileges.
2. From the workspace navigation panel, select **Configuration** workspace.
3. Select **Quality Assurance Configuration Console**.

   The console opens.
4. In the **Configuration** workspace, select **Site Based Threshold**

   The Threshold Configuration form opens.

Threshold Configuration Process

This section describes all the typical interactions that take place between the actor and this use case.

Format: If the actor selects `<selection>`, the system will request the actor to enter information.

Perform the following steps to add a new threshold to a site:

1. Launch the Threshold Configuration form. See "Threshold Configuration Process" (on page 124).
2. Click  **New** in the Site Wide Threshold Settings panel.

   The Add Threshold Configuration form opens.
3. Specify the following information in the Threshold Configuration panel:

Field Name	Description
Source Site	Select `SiteA`.
Destination site	Select `SiteB`.
Service Type	Select `VoIP`.

   The new threshold you create is automatically assigned to the QA probes initiated from `SiteA` and run on the network elements in `SiteB`.
4. Click  **New** in the Threshold Settings panel.

   The Add Threshold Settings form opens.

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

Field Name	Description
Type	Count Based
Metric	Two Way Jitter(µsecs)
High Value	75
High Value Rearm	70
Trigger Count	2
Generate Incident	Select this option

6. Click  **Save and Close**

   The Add Threshold Settings form closes.

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

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

Process Termination

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

Exceptions

- You cannot create threshold settings if you do not have at least one site.
- If you do not select a destination site for the threshold settings, the settings will be applied to all the QA probes initiated from the source site.
- The new threshold will not be saved unless you click  **Save and Close** in the Add Threshold Settings form.

Post Conditions

- The threshold settings are applied to the poller immediately once you complete creating a threshold.
- The HP Network Node Manager iSPI Performance for Quality Assurance Software applies the threshold for Two Way Jitter(µsecs) on all the QA probes run from SiteA and on SiteB.
- The NNM iSPI Performance for QA generates an incident if the Two Way Jitter(µsecs) crosses the high threshold value of 75 for two consecutive times.
- The Jitter column of the QA Probes view displays a **High** state.
- The Incident tab in the QA Probes form displays a **Critical** incident raised on the network element if an incident is raised.
- The Threshold State tab in the QA Probes form the threshold displays a **High** state.
- The Status tab in the QA Probes form displays the network element status as **Major**.
- The NNM iSPI Performance for QA clears the generated incident when the Two Way Jitter(µsecs) reaches the high value rearm of 70.
- The Incident tab in the QA Probes form reflects the change when an incident is cleared.
- The Threshold State tab in the QA Probes form the threshold displays a **Nominal** state.
- The Status tab in the QA Probes form displays the network element status as **Normal**.

You can view the threshold violated probes in the Threshold Exceptions probe view. In addition, you can view the report of the threshold violated probes view in the Network Performance server.

QA Probes Form: Incidents Tab

The QA Probes form contains details about the selected QA probe from the QA Probes Inventory view.

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

The NNM iSPI Performance for QA supports multitenant architecture configured in NNMi. A user can view the incidents only if the source node can be accessed by the user.

Attribute: Incidents Tab

Attribute	Description
Incidents Attributes	The attributes listed in the incidents tab are same as available in the NNMi Incidents form. For more information for the attributes, see the topic *NNMi Incidents Form* in the *Network Node Manager i SoftwareOnline help* HP Network Node Manager iSPI Performance for Quality Assurance Software generates the following incidents: TwoWayJitterHigh Indicates high two way jitter. This value is the average of the following values: • Positive jitter from the source to the destination

Attribute	Description
	• Negative jitter from the source to the destination • Positive jitter from the destination to the source • Negative jitter from the destination to the source
	SourceToDestinationPositiveJitterHigh Indicates high positive jitter from the source to the destination, based on the reported value on the MIB. The exact MIB values that are queried vary based on whether the latest value is polled or cumulative value is polled.
	DestinationToSourcePositiveJitterHigh Indicates high positive jitter from the destination to the source, based on the reported value on the MIB. The exact MIB values that are queried vary based on whether the latest value is polled or cumulative value is polled.
	SourceToDestinationNegativeJitterHigh Indicates high negative jitter from the source to the destination, based on the reported values on the MIB. The exact MIB values that are queried vary based on whether the latest value is polled or cumulative value is polled.
	DestinationToSourceNegativeJitterHigh Indicates high negative jitter from the destination to the source, based on the reported values on the MIB. The exact MIB values that are queried vary based on the whether the latest value is polled or cumulative value is polled.
	TwoWayPacketLossHigh Indicates high percentage of two way packet loss. This value is the average of the following values: • Packet loss percentage from the source to the destination • Packet loss percentage from the destination to source
	SourceToDestinationPacketLossHigh Indicates high percentage of packet loss from the source to the destination. The packet loss percentage is calculated based on the total number of packets sent and the reported number of packets lost. The exact MIB values that are queried vary based on whether the latest value is polled or cumulative value is polled.
	DestinationToSourcePacketLossHigh Indicates high percentage of packet loss from the destination to the source. The packet loss percentage is calculated based on the total number of packets sent and the reported number of packets lost. The exact MIB values that are queried vary based on whether the latest value is polled or cumulative value is polled.

Attribute	Description
	RoundTripTimeHigh Indicates high round trip time, based on the reported value on the MIB. The exact MIB values that are queried vary based on whether the latest value is polled or cumulative value is polled.
	MeanOpinionScoreLow Indicates low mean opinion score, based on the reported value on the MIB. The exact MIB values that are queried vary based on whether the latest value is polled or cumulative value is polled.
	RoundTripTimeAbnormal Indicates round trip time is of Abnormal range. This implies the RTT is above the configured normal range of the deviation.
	TwoWayPacketLossAbnormal Indicates two way packet loss is of Abnormal range. This implies the two way packet loss is above the configured normal range of the deviation. This value is the average of the following values: • Packet loss percentage from the source to the destination • Packet loss percentage from the destination to source
	TwoWayJitterAbnormal Indicates two way jitter is of Abnormal range. This implies the two way jitter is above the configured normal range of the deviation. This value is the average of the following values: • Positive jitter from the source to the destination • Negative jitter from the source to the destination • Positive jitter from the destination to the source • Negative jitter from the destination to the source
	MeanOpinionScoreAbnormal Indicates Mean Opinion Score is of Abnormal range. This implies the mean opinion score is either above or below the configured normal range of the deviation.
	TestError This incident indicates that the QA Probe has returned an error.
	TestTransient This incident indicates that the QA Probe is in transient state.
	TestFailed This incident indicates that the QA Probe has failed to run.
	TestDisabled This incident indicates that the QA Probe is explicitly disabled by the device administrator.

QA Probes Form: State Tab

The QA Probes form contains details about the selected QA probe from the QA Probes Inventory view.

The State tab displays information about the last run of the QA probe.

Attributes: State Tab

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

QA Probes Form: Status Tab

The QA Probes form contains details about the selected QA probe from the QA Probes Inventory view.

The Status tab displays a quick summary of the SPI object status to better determine and monitor any significant patterns in behavior and activity.

Attribute: Status Tab

Attribute	Description
Status	Overall status for the current QA probe Possible values are as follows: • No Status • Normal • Disabled • Unknown • Warning • Major • Critical For more information on the QA probe status, see the topic QA Probe Status

Attribute	Description
	Note: In the case of sub-minute polling, the QA probe status refreshes every 2 minutes. The QA probe status gets updated based on the average polling value obtained for the last 2 minutes. See the following topics for information about how the current status was determined: • QA Probes Form: State Tab • QA Probes Form: Conclusions Tab
Status Last Modified	Current status is calculated and set by Causal Engine. The Time Stamp data displays the time when the status of the QA probe is last updated.
Status History	List of up to the last 30 changes in status for the selected QA probe. This view is useful for obtaining a summary of the QA probe status so that you can better determine any patterns in traffic between the source node or site and the destination node or site. **Note:** • Click  **Refresh** to refresh the Status History table. • Click  **Show View in New Window** to open the Status History table in an independent window.

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 console

HP Network Node Manager iSPI Performance for Quality Assurance Software Help for Operators

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

- Discover the QA probes configured in the nodes managed by NNMi
- Configure QA probes
  (User with administrator or Level 2 Operator privileges can only configure probes)
- Monitor the network performance and view the threshold state of the metric in the NNMi console
- Analyze the outcome of each QA probe and generate reports upto a maximum period of 13 months

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 monitors the network performance at the packet level with the following metrics:

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

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

NNM iSPI Performance for QA enables to monitor the network performance for the devices that support the following MIBS:

- CISCO-RTTMON-MIB
- DISMAN-PING-MIB
- JNX-RPM-MIB

NNM iSPI Performance for QA supports the following vendor- specific technologies:

- CISCO IP SLA
- JUNIPER RPM
- Other vendors supporting the DISMAN Ping using RFC 4560

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

- UDP Echo
- ICMP Echo
- UDP

- TCP Connect
- VoIP

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

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

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

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

You can then view the following:

NNM iSPI Performance for QA workspace: Access the QA Probes view to view the status and other details for the pre-configured QA probes on the nodes managed by NNMi. In addition, you can access the Threshold Exceptions Probes view, Critical Probes View, and Baseline Exceptions Probes View to view a specific set of QA probes.

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

HP Network Node Manager iSPI Performance for Quality Assurance Software Multitenancy

Multitenant Architecture in NNM iSPI Performance for QA

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

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

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

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

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

Multitenant architecture establishes a node to tenant association and determines the nodes that can be accessed by the user. However, you can configure the QA probes for a source node irrespective of whether you can access the destination node. A user with administrator privileges or Level 2 Operator access can configure probes.

An administrator can create, update, and delete all configurations whereas other users can only view the configuration details, and no multitenancy is required as the configuration is allowed based on the user group.

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

Accessing the Quality Assurance Workspace

After you install HP Network Node Manager iSPI Performance for Quality Assurance Software, a new workspace for Quality Assurance gets added to your NNMi console.

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

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

To launch the Quality Assurance workspace:

1. Log on to NNMi console using your 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 Software Online Help* for more information

2. Click **Quality Assurance** in the Workspaces panel. The Quality Assurance tab expands, displaying the QA Probes view, Critical Probes view, Threshold Exceptions Probes view, and Baseline Exceptions Probes view.

Managing the Quality Assurance Workspace

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

Task Options to Manage the Quality Assurance Workspace

Icons	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.
 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.
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 Inventory Views

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 equals `<value>`	• Is Empty • Not Empty	No lowest value	No highest 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	No disallowed filter	No lowest value	No highest value

	• Not Empty			
RTT	• Equals <value> • Not equals <value> • Is Empty • Not Empty	• Contains • Matches	0	Not Applicable
Jitter	• Equals <value> • Not equals <value> • Is Empty • Not Empty	• Contains • Matches	0	Not Applicable
Packet Loss	• Equals <value> • Not equals <value> • Is Empty • Not Empty	• Contains • Matches	0	Not Applicable
Manager	• Equals <value> • Not equals <value> • Is Empty • Not Empty	No disallowed filter	No lowest value	No highest value

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) 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) 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 Inventory Views

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

Sorting is enabled only for limited columns.

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

To sort a column in the Quality Assurance workspace, right click 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 Inventory View

The QA Probes view displays all the QA probes configured in the network elements. The QA probes are discovered by the 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. Click the QA Probes view to display the QA probes discovered in your network.

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

Apart from the menu bar, you can perform some of the actions by following the step below:

Right click on the probe(s), and select **Quality Assurance** option and the required sub-menu to perform the action.

Key Attributes of the QA Probes View

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

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

Attribute Name	Description
Status	The status that the QA probe returned. A QA probe may return any of the following statuses : • Normal • Warning • Major • Critical • Unknown • Disabled • Not Polled • No Status For more information on status, see the topic QA Probe Status
Name	The name of the discovered QA probe configured in the network device
Owner	The name of the discovered QA probe's owner.

Attribute Name	Description
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 recognizes are as follows: • UDP Echo • ICMP Echo • UDP • TCP Connect • VoIP
Source	The source device in which the probe is configured
Destination	The destination network device till which the probe is configured
Source Site	The source site to which the configured probe is associated.
Destination Site	The destination site to which the configured probe is associated.
RTT	The round-trip time used by the selected QA probe Displays any one of the following threshold states for the metric High Nominal Low Not Polled Unavailable Threshold Not Set None
Jitter	The delay variance for a data packet to reach the destination device or site Displays any one of the following threshold states for the metric High Nominal Low Not Polled Unavailable Threshold Not Set None

Attribute Name	Description
PL (Packet Loss)	The percentage of packets that failed to arrive at the destination. Displays any one of the following threshold states for the metric High Nominal Low Not Polled Unavailable Threshold Not Set None
Manager	Specifies whether the NNMi management server is Local or specifies the name of the Regional Manager.

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

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

Threshold States

State	Description
High	*For Count Based Threshold Configuration:* Indicates that the measured value of the metric is above the configured High Value and recurs for the consecutive number of times specified in the Trigger Count *For Time Based Threshold Configuration:* Indicates that the measured value of the metric is above the configured High Value and this high value persists for the specified High Duration within the High Duration Window
Nominal	Indicates that the measured value of the metric is within the normal healthy range
Low	*For Count Based Threshold Configuration*: Indicates that the measured value of the metric is below the configured Low Value for the consecutive number of times specified in the Trigger Count *For Time Based Threshold Configuration:* Indicates that the measured value of the metric is below the configured Low Value and this low value persists for the specified Low Duration within the Low Duration Window. Note: Typically, this threshold state is applicable for metrics like Mean Opinion Score (MOS)

State	Description
Not Polled	Indicates that the 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 the valid range
Threshold Not Set	Indicates that the threshold is not set for the metric
None	*For Count Based Threshold Configuration:* Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count *For Time Based Threshold Configuration:* Indicates that the measured value of the metric is zero and this zero value persists for the specified duration within the High or Low Duration Window (depending on the metric).

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

Analysis Pane

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

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

The summary includes details such as the Status of the QA probe, Conclusions, Name of the QA probe, Service Type, TOS value, Frequency (Polling Interval), and the VRF. You can view the conclusions of the threshold violations in the summary.

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

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

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

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

Related Topics

Manage the Quality Assurance Workspace

Sort Data in the QA Probes View

Filter Data in the QA Probes View

Launch the QA Probe Forms

QA Probe Status

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

Status	Description for Operators	Description for Administrators
Normal	The source node is Ok or Enabled	The source node or site is Active or Enabled
Warning	The source node has returned any of the following status: • Other • Disconnected • Over the threshold value • Busy • Not Connected • Dropped	The source node or site is Active or Enabled
Major	Indicates the metric in QA probe breaches the threshold level.	Indicates the metric in QA probe breaches the threshold level.
Critical	The source node has returned any of the following errors: • Timed out error • Sequence error • Verify error • Application specific error • DNS server timeout error • TCP connect timeout error	The source node or site has returned any of the following status: • Not ready • Create and go • Create and wait • Destroy

Status	Description for Operators	Description for Administrators
	• HTTP transaction timeout error • DNS query error • HTTP error • State error • Source node or site disabled	
Unknown	The source node has returned any of the following errors: • SNMP error • If there is no polling policy	The source node or site is Active or Enabled
Disabled	The source node is disabled	The source node or site has returned any of the following status: • Not in service • Disabled
Not Polled	When the user selected not to poll the source node	When the user selects not to poll the source node

Status	Description for Operators	Description for Administrators
No Status	• When the node is not managed – Indicates the node is intentionally not managed. For example, certain nodes may not be managed during scheduled network maintenance cycles. HP Network Node Manager i Software does not update discovery information or monitor these nodes. • When the node is out of service – Indicates a node is unavailable because it is out of service. NNMi does not update discovery information or monitor these nodes. This attribute is useful for notifying NNMi when a device has been temporarily out of service, or should never be managed.	• When the node is not managed – Indicates the node is intentionally not managed. For example, certain nodes may not be managed during scheduled network maintenance cycles. NNMi does not update discovery information or monitor these nodes. • When the node is out of service – Indicates a node is unavailable because it is out of service. NNMi does not update discovery information or monitor these nodes. This attribute is useful for notifying NNMi when a device has been temporarily out of service, or should never be managed.

Accessing the Critical QA Probes Inventory View

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

To launch the Critical Probes view:

1. Log on to NNMi console using your username and password.
2. Click **Quality Assurance** in the Workspaces panel. The Quality Assurance tab expands.
3. Click **Critical Probes** to display the QA probes of Critical status that are discovered in your network.

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

Key Attributes of the Critical Probes View

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

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

Attribute Name	Description
Operational State	Operational State condition returned by the critical QA probe The QA probe status is derived from the SNMP polling results for Operational State, as well as from any conclusion.

Attribute Name	Description
Administrative State	Administrative State condition returned by the QA probe The QA probe status is derived from the SNMP polling results for Administrative State, as well as from any conclusion.
Name	The name of the discovered QA probe configured in the network device.
Owner	The name of the discovered QA probe's owner.
Service	The type of the discovered QA probe. Some of the QA probe types that the HP Network Node Manager iSPI Performance for Quality Assurance Software recognizes are as follows: • UDP Echo • ICMP Echo • UDP • TCP Connect • VoIP
Source	The source device from which the data packet is sent.
Destination	The network device to which the data packet is sent.
Source Site	The network site from which the data packet is sent.
Destination Site	The network site to which the data packet is sent.
Manager	Specifies whether the NNMi management server is Local or specifies the name of the Regional Manager.

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

Analysis Pane

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

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

The summary includes details such as the Status of the QA probe, Conclusions, Name of the QA probe, Service Type, TOS value, Frequency (Polling Interval), and the VRF. You can view the conclusions of the threshold violations in the summary.

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

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

Administrative State

The following table describes the different Administrative State for IP SLA and RFC QA probes:

Cisco IP SLA QA Probe State Attributes	Description
rttMonCtrlAdminStatus	The status of the conceptual RTT control row. The current Administrative State contributes towards the status calculation for this QA probe. Possible values are: • active Indicates that the conceptual row is available for use by the managed device • notInService Indicates that the conceptual row exists in the agent, but is unavailable for use by the managed device. • notReady Indicates that the conceptual row exists in the agent, but is missing information necessary in order to be available for use by the managed device. • createAndGo Supplied by a management station wishing to create a new instance of a conceptual row and to have its status automatically set to active, making it available for use by the managed device. • createAndWait Supplied by a management station wishing to create a new instance of a conceptual row (but not make it available for use by the managed device). • destroy Supplied by a management station wishing to delete all of the instances associated with an existing conceptual row.

RFC QA Probe or Juniper RPM QA Probe State Attributes	Description
pingCtlAdminStatus	For RFC the following values are supported for the Administrative State: • Enabled Attempt to activate the QA probe.

	• Disabled Deactivate the QA probe.

Operational State

The following table describes the different Operational State for IP SLA and RFC QA probes:

Cisco IP SLA QA Probe State Attributes	Description
• rttMonLatestJitterOperSense • rttMonLatestRttOperSense	The rttMonLatestJitterOperSense status defines an application specific sense code for the completion status of the latest Jitter RTT operation. The rttMonLatestRttOperSense status defines an application sense code for the completion status of the latest RTT operation. The current Operational State contributes towards the status calculation for this QA probe. Possible values are: • other(0) The operation is not started or completed or this object is not applicable for the probe type. • ok(1) A valid completion occurred and timed successfully. • disconnected(2) The operation did not occur because the connection to the target was lost. • overThreshold(3) A valid completion was received but the completion time exceeded a threshold value. • timeout(4) An operation timed out; no completion time recorded. • busy(5) The operation did not occur because a previous operation is still outstanding. • notConnected(6) The operation did not occur because no connection (session) exists with the target.

Cisco IP SLA QA Probe State Attributes	Description
	• dropped(7) The operation did not occur due to lack of internal resource. • sequenceError(8) A completed operation did not contain the correct sequence id; no completion time recorded. • verifyError(9) A completed operation was received, but the data it contained did not match the expected data; no completion time recorded. • applicationSpecific(10) The application generating the operation had a specific error. • dnsServerTimeout(11) DNS Server Timeout • tcpConnectTimeout(12) TCP Connect Timeout • httpTransactionTimeout(13) HTTP Transaction Timeout • dnsQueryError(14) DNS Query error (because of unknown address etc.) • httpError(15) HTTP Response StatusCode is not OK (200) then HTTP error is set. • error(16) If there are socket failures or some other errors not relevant to the actual probe, they are recorded under this error.

RFC QA Probe or Juniper RPM QA Probe State Attributes	Description
pingResultsOperStatus	For RFC the following values are supported for the Operational State: • Enabled QA probe is active. • Disabled QA probe has stopped.

Accessing the Threshold Exceptions Probes Inventory View

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

The QA Probes view just gives an overview of the violation of the threshold state for the metrics such as Jitter, RTT and so on. However, the Threshold Exceptions Probes view is very exhaustive, and displays the intricate details of violation of the threshold states such as Positive Jitter or Negative Jitter, and so on. This view is very useful to segregate the QA probes that have violated the threshold state and arrive at a conclusion.

To launch the Threshold Exceptions 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
3. Click **Threshold Exceptions Probes** to view the QA probes that has violated the threshold for Jitter, RTT, Packet Loss and Mean Opinion Score metrics.

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

Each QA probe displays information for a specific time interval.

Note: The default time interval to refresh is 300 seconds, or 5 minutes. You can generate reports in the Network Performance Server for the threshold violated probes.

Key Attributes of the Threshold Exceptions Probes View

Attribute Name	Description
Status	Displays the QA probes of the following status: • Warning • Major • Critical

Attribute Name	Description
	For more information on status, see the topic QA Probe Status
Name	The name of the discovered QA probe configured in the network device.
Service	The type of the discovered QA probe. Some of the QA probe types that the HP Network Node Manager iSPI Performance for Quality Assurance Software recognizes are as follows: • UDP Echo • ICMP Echo • UDP • TCP Connect • VoIP
Manager	Specifies whether the NNMi management server is Local or specifies the name of the Regional Manager.
RTT	The round-trip time used by the selected QA probe. Displays any one of the following threshold states for the metric High Nominal Low Not Polled Unavailable Threshold Not Set None
Jitter	The delay variance for a data packet to reach the destination device or site. Displays any one of the following threshold states for the metric High Nominal Low Not Polled Unavailable Threshold Not Set None

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

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

Attribute Name	Description
Packet Loss DS	Indicates the threshold state of the percentage of packet loss from the destination to source. Displays any one of the following threshold states for the metric High Nominal Low Not Polled Unavailable Threshold Not Set
MOS	Indicates the threshold state of the Mean Opinion Score (MOS) of the jitter.

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

Threshold States

State	Description
High	*For Count Based Threshold Configuration:* Indicates that the measured value of the metric is above the configured High Value and recurs for the consecutive number of times specified in the Trigger Count *For Time Based Threshold Configuration:* Indicates that the measured value of the metric is above the configured High Value and this high value persists for the specified High Duration within the High Duration Window
Nominal	Indicates that the measured value of the metric is within the normal healthy range
Low	*For Count Based Threshold Configuration*: Indicates that the measured value of the metric is below the configured Low Value for the consecutive number of times specified in the Trigger Count *For Time Based Threshold Configuration:* Indicates that the measured value of the metric is below the configured Low Value and this low value persists for the specified Low Duration within the Low Duration Window. Note: Typically, this threshold state is applicable for metrics like Mean Opinion Score (MOS)
Not Polled	Indicates that the metric is intentionally not polled. Some of the possible reasons are:

State	Description
	• 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 the valid range
Threshold Not Set	Indicates that the threshold is not set for the metric
None	*For Count Based Threshold Configuration:* Indicates that the measured value of the metric is zero, and recurs for the consecutive number of times specified in the Trigger Count *For Time Based Threshold Configuration:* Indicates that the measured value of the metric is zero and this zero value persists for the specified duration within the High or Low Duration Window (depending on the metric).

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

Analysis Pane

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

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

The summary includes details such as the Status of the QA probe, Conclusions, Name of the QA probe, Service Type, TOS value, Frequency (Polling Interval), and the VRF. You can view the conclusions of the threshold violations in the summary.

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

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

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

Accessing the Baseline Exceptions Probes Inventory View

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

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

For more information, see the topic Baseline Monitoring

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

To launch the Baseline Exceptions 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
3. Click **Baseline Exceptions Probes** to view the QA probes with the baseline state as Abnormal Range, Unavailable, or Not Polled for any one or more of the metrics.

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

Each QA probe displays information for a specific time interval.

Note: The default refresh time interval is 300 seconds, or 5 minutes.You can generate reports in the Network Performance Server for the probes with baseline exceptions.

Key Attributes of the Baseline Exceptions Probes View

Attribute Name	Description
Status	Displays the QA probes of the following status: • Normal • Warning • Major • Critical • Unknown • Disabled • Not Polled • No Status For more information on status, see the topic QA Probe Status
Name	The name of the discovered QA probe configured in the network device.
Service	The type of the discovered QA probe. Some of the QA probe types that the HP Network Node Manager iSPI

Attribute Name	Description
	Performance for Quality Assurance Software recognizes are as follows: • UDP Echo • ICMP Echo • UDP • TCP Connect • VoIP
Manager	Specifies whether the NNMi management server is Local or specifies the name of the Regional Manager.
RTT	The round-trip time used by the selected QA probe. Displays any one of the following baseline states for the metric: • Normal Range - The metric is within the normal range of deviation • Abnormal Range - The metric is above the configured normal range of the deviation • Unavailable - The computed value for the metric is not found in HP NNM iSPI Performance for Metrics Software • Unset - No baseline is computed • Not polled - The metric is not polled for baseline deviations • No Policy - No polling policy exists for this metric
Two Way Jitter	Indicates two way jitter. This value is the average of the following values: • Positive jitter from the source to the destination • Negative jitter from the source to the destination • Positive jitter from the destination to the source • Negative jitter from the destination to the source Displays any one of the following baseline states for the metric: • Normal Range - The metric is within the normal range of deviation • Abnormal Range - The metric is either above or below the configured normal range of the deviation • Unavailable - The computed value for the metric is not found in HP NNM iSPI Performance for Metrics Software • Unset - No baseline is computed • Not polled - The metric is not polled for baseline deviations

Attribute Name	Description
	• No Policy - No polling policy exists for this metric
Two Way Packet Loss	The percentage of packets that failed to arrive from the source to destination and destination to source. Displays any one of the following baseline states for the metric: • Normal Range - The metric is within the normal range of deviation • Abnormal Range - The metric is either above or below the configured normal range of the deviation • Unavailable - The computed value for the metric is not found in HP NNM iSPI Performance for Metrics Software • Unset - No baseline is computed • Not polled - The metric is not polled for baseline deviations • No Policy - No polling policy exists for this metric
MOS	Indicates the baseline state of the Mean Opinion Score (MOS) of the jitter. Displays any one of the following baseline states for the metric: • Normal Range - The metric is within the normal range of deviation • Abnormal Range - The metric is either above or below the configured normal range of the deviation • Unavailable - The computed value for the metric is not found in HP NNM iSPI Performance for Metrics Software • Unset - No baseline is computed • Not polled - The metric is not polled for baseline deviations • No Policy - No polling policy exists for this metric

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

Analysis Pane

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

Launching the Forms

To launch the forms:

1. From the left navigation panel, select the **Quality Assurance** Workspace and select any one of the views. The valid views are QA Probes View, Critical Probes View, Threshold Exception Probes View, and Baseline Exception 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 Probe Form

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

QA Probe Form: Left Panel

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

QA Probe Details

This section displays the following:

Basic Attributes: QA Probe Details

Attribute	Description
Status	Status of the QA probe. A QA probe can have any of the following status: • No Status • Normal • Disabled • Unknown • Warning • Major • Critical For more information on the status, see the topic Key Status Displayed in the QA Probes View
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.

Attribute	Description
Owner	Name of the QA probe owner
Service	Type of the QA probe Possible service types are: • UDP Echo • ICMP Echo • UDP • TCP Connect • VoIP
Admin Index	The unique index ID given for each QA probe Available only for Cisco IP SLA QA probes.
Manager	Specifies whether the NNMi management server is Local or specifies the name of the Regional Manager.

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

Attribute	Description
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 stopping 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
VRF	Virtual Routing and Forwarding (VRFs) tables defined on the source node. This field is populated only if the test is configured with VRF(s).
Discovery State	Discovered state of the source node Possible values are as follows: Completed - All the analysis are completed and the QA probes are discovered. In Progress- The discovery process is still gathering network information or the QA probe data.
Last Discovery Completed	Date, time, and time zone for the last discovery
Management Mode	Whether the source node is managed or not Possible states are as follows: • Managed • Unmanaged • Unknown

Probes Form: Right Panel

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

- State
- Threshold State
- Baseline State
- Jitter Configuration
- Status

- Conclusions
- Incidents
- Registration

Analysis Pane

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

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

The summary includes details such as the Status of the QA probe, Conclusions, Name of the QA probe, Service Type, TOS value, Frequency (Polling Interval), and the VRF. You can view the conclusions of the threshold violations in the summary.

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

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

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

Related Topics

Accessing the QA Probes View

Accessing the Critical QA Probes View

Accessing the Threshold Exceptions Probes View

Accessing the Baseline Exceptions Probes View

Viewing Source Interface for a QA Probe

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

The NNM iSPI Performance for QA maps the interface only if the HP Network Node Manager i Software 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 QA probes, specify the source IP address to the QA probe.
- For RFC 4560 QA or Juniper RPM probes, specify the source interface index when configuring the QA probes.
- You can also use the Probe Configuration form. For more information,see Configure Probes

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

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

1. Click  next to the Source Interface in the QA Probes form.
2. Select **Open**.

   The Interface form opens.
3. Select **Actions** and **Reporting - Report Menu** to display the reports related to the interface.

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.

HP Network Node Manager iSPI Performance for Quality Assurance Software Site Map

You can view the performance of a network in a QA probe inventory view or form view. However, in a large enterprise networks, you need to assess the performance of each site, and monitor the overall network performance. Site Map enables you to easily identify the performance of any site and gives a holistic view of the network.

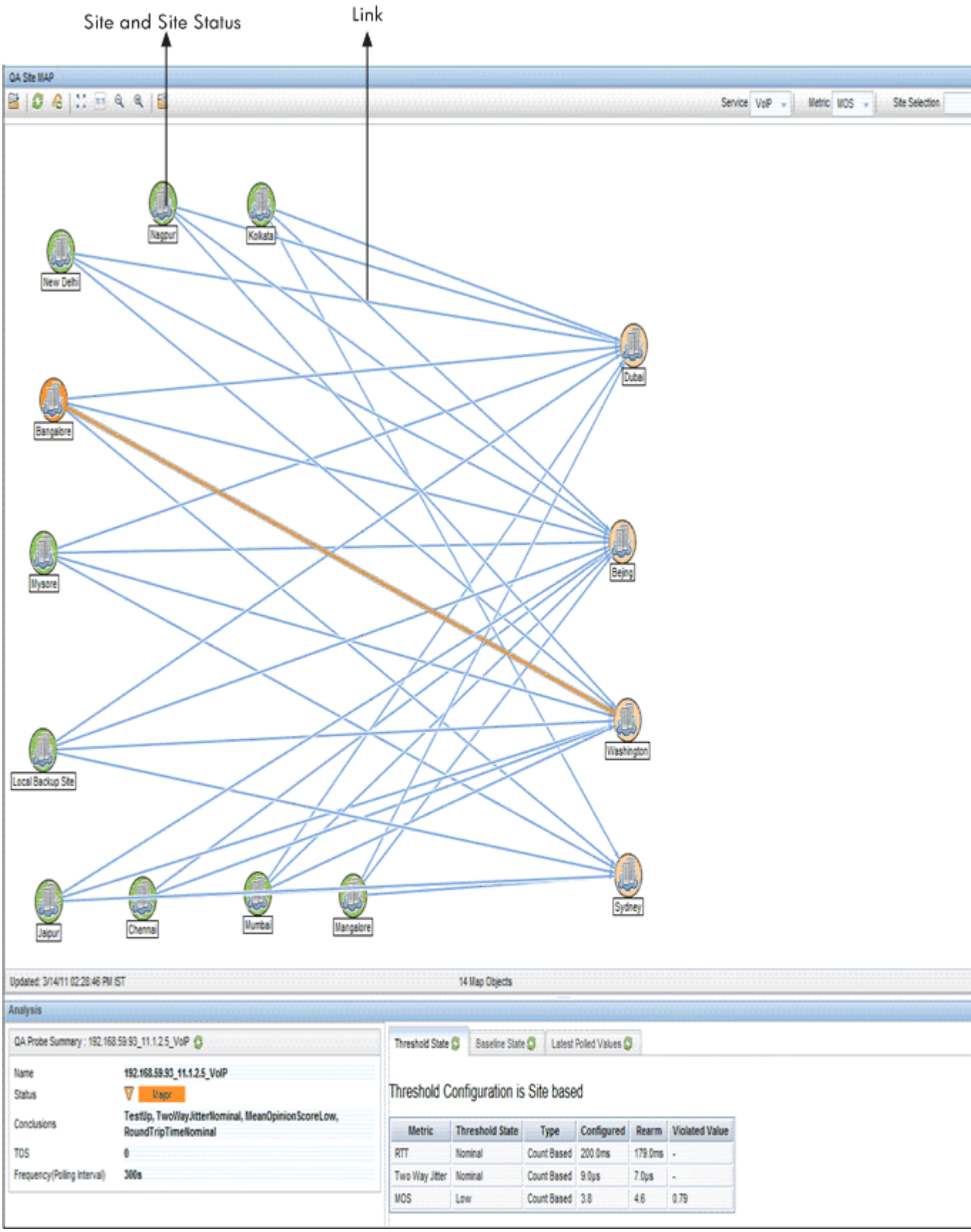
The site map represents the sites as nodes, and the most severe probe status as links between the sites.

You can understand the terminologies used in site map by referring to the following table:

Terminology	Description
Site Status	The status and coloring scheme of a site is derived based on the **most severe operational status** of all the QA probes originating from the source site for the selected service, and metric.
Links	Links are unidirectional for the QA probes originating from the source to destination site. The color of the link is based on the threshold state of the probe for the selected service and metric. Note: In the case of a two-way jitter, the link color is based on the

Terminology	Description
	threshold state of the metric in the source, and destination sites

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


Site and Site Status
Link
QA Site MAP
Service VoIP
Metric MOS
Site Selection
Nagpur
Kolkata
New Delhi
Dubai
Bangalore
Mysore
Beijing
Washington
Local Backup Site
Jaipur
Chennai
Mumbai
Mangalore
Sydney
Updated: 3/14/11 02:28:46 PM IST
14 Map Objects
Analysis
QA Probe Summary : 192.168.59.93_11.1.2.5_VoIP
Name 192.168.59.93_11.1.2.5_VoIP
Status Major
Conclusions TestUp, TwoWayJitterNominal, MeanOpinionScoreLow, RoundTripTimeNominal
TOS 0
Frequency(Polling Interval) 300s
Threshold State
Baseline State
Latest Polled Values
Threshold Configuration is Site based
Metric | Threshold State | Type | Configured | Rearm | Violated Value
RTT | Nominal | Count Based | 200.0ms | 179.0ms | -
Two Way Jitter | Nominal | Count Based | 9.0µs | 7.0µs | -
MOS | Low | Count Based | 3.8 | 4.6 | 0.79

The data is retrieved from NNM iSPI Performance for QA, and you can view the site map in the NNMi console.

The NNM iSPI Performance for QA supports multitenant architecture configured in NNMi. A user can view the site map only if atleast one of the QA probes of the source site can be accessed by the user.

Site status and the overall view of the site map varies based on whether the user has access to a set of probes in a site. If a user can access a set of probes in a site, the site status appears based on the overall status of those probes in a site, which may be different for another user.

You can refer to the following table to understand the coloring scheme for the site status or the QA probe status:

Site Status Color	Operational Status Description
Gray	No Status/Disabled/Warning
Green	Normal
Blue	Unknown
Orange	Major
Red	Critical

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

You can refer to the following table to understand the coloring scheme of the link or the Threshold state:

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

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

Related Topics

Launching the Site Map

Launching the Site Map

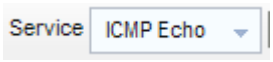
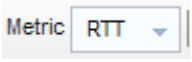
To launch the site map, follow these steps:

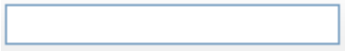
1. Log on to NNMi console using your username and password.
2. Select **Action** → **Quality Assurance** → **Site Map** from the NNMi console to view the site map.
3. Select the service from the **Service** drop-down list. By default, NNM iSPI Performance for QA populates the `ICMP Echo` service. See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

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

The site map automatically refreshes every five minutes.

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

Icons Available in the Site Map Toolbar	Description
 Open	Opens the selected site details
 Refresh	Refreshes the view, site status and link status in the site map
 Refresh Status	Refreshes only the site status in the site map
 Service	Select any one of the following Services from the drop-down list for which you intend to view the site map: • UDP Echo • ICMP Echo • UDP • TCP Connect • VoIP By default, NNM iSPI Performance for QA populates the `ICMP Echo` Service.
 Metric	Select any one of the following metrics from the drop-down list for which you intend to view the site map:

Icons Available in the Site Map Toolbar	Description
	• RTT • + ve Jitter • -ve Jitter • TwoWay Packet Loss • TwoWay Jitter • MOS By default, NNM iSPI Performance for QA populates the `RTT` Metric Type. Note: +ve and -ve Jitter are always from source to destination in the site map. +ve Jitter, -ve Jitter, and TwoWay Jitter metrics are applicable only for UDP and VoIP service. The Mean Opinion Score (MOS) metric is applicable only for VoIP service.
 Site Selection	Type the name of the site or the search string of the sites, and click  to view a specific set of sites in the site map . You can enter the site name partially with the wild card asterisk "*" (to replace any number of characters) to retrieve all the sites based on the search string. For example, if you intend to view all the sites starting with `Ban`, you need to enter `Ban*` in the search string. Also, you can use the wild card "?" to replace one character in the search string. For example, if you intend to view the sites starting with any one character followed by the string `angalore`, you need to enter `*angalore` in the search string. You can also use a combination of the wildcard * and ? in the search string. Note: This search for the sites is **case-sensitive**.

Icons Available in the Site Map Toolbar	Description
Launch	Launches the site map based on the selection. Note: The site map also launches for the sites which have no destination sites.
Find	Displays a drop-down list where you can select the site which you want to find in the site map.

Click here to view a typical site map.

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

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

Analysis Pane

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

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

Related Topics

Overview of Site Map

HP Network Node Manager iSPI Performance for Quality Assurance Software Real Time Line Graph

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

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

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

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

Related Topics

Launching the Real Time Line Graph

Launching the Real Time Line Graph

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

1. Log on to NNMi console using your username and password.
2. You can either launch the graph for the QA probes configured on the node, or you can launch the graph for selected QA probes from any one of the following Inventory views:

   QA Probes View

   Critical Probes View

   Threshold Exceptions Probe View

   Baseline Exception Probes View
3. To launch the graph for QA probes configured on a node, follow these steps:

   a. Click **Inventory** in the Workspaces panel.
   The **Inventory** tab expands.

   b. Click **Nodes**, and the Node view appears.
   Select the node for which you need to view the Real Time Line graph.

   c. Select **Actions** → **Quality Assurance** → **Graph** → **<Service>** → **<metric name>** → **<metric sub menu>**
4. Alternatively, to launch the graph for selected QA probes, follow these steps:
   a. Click **Quality Assurance** in the Workspaces panel. The Quality Assurance tab expands, displaying the **QA Probes** view.

   b. Select the QA probes for which you require to view the Real Time Line graph.

   c. Select **Actions** → **Quality Assurance** → **Graph** →**<metric name>** → **<metric sub menu>**

   Note: If a node has numerous probes configured, it is recommended you launch the Real Time Line graph for selected probes rather than launching the Real Time Line graph for a node. This facilitates you to make use of the Real Time Line graph effectively.
5. The following table lists the valid **service**, **metric name** and the **metric sub menu**:

Service	Metric Name	Metric Sub Menu
UDP or TCP or VOIP	Jitter	▪ Negative Jitter DS ▪ Negative Jitter SD ▪ Positive Jitter DS ▪ Positive Jitter SD ▪ Two Way Jitter Note: DS is the acronym for Destination to Source and SD is the acronym for Source to Destination.
	Packet Loss	▪ Packet Loss DS ▪ Packet Loss SD ▪ Two Way Packet Loss Note: DS is the acronym for Destination to Source and SD is the acronym for Source to Destination.
	Round Trip Time	▪ Average RTT in Milliseconds ▪ Average RTT in Microseconds
	Mean Opinion Score Note: This option appears only for VOIP service	
ICMP Echo	Round Trip Time	▪ Average RTT in Milliseconds ▪ Average RTT in Microseconds
UDP Echo	Round Trip Time	▪ Average RTT in Milliseconds ▪ Average RTT in Microseconds

The Real Time Line Graph appears. Note that in a Global Network Management environment, you cannot view the Real Time Line graph for the Remote QA Probes.

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

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

The Juniper RPM devices supports the following metrics:

- Negative Jitter DS
- Negative Jitter SD
- Positive Jitter DS

- Positive Jitter SD
- Two Way Packet Loss
- Average RTT in Milliseconds

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

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

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

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

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

7. You can select the polling interval:

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

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

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

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

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

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

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

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

Related Topics

Overview of Real Time Line Graph

HP Network Node Manager iSPI Performance for Quality Assurance Software QA Application Health Report

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

Launching the QA Application Health Report

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

The user interface displays seven tabs; Memory, CPU Usage, System, Database, Site Associations, StatePoller, and GNM

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

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

The **CPU Usage** tab displays the following information only for UNIX platforms:

- CPU Utilization
- Load Average

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

- Available Processors
- Free Physical Memory
- Physical Memory
- Committed Virtual Memory

- Free Swap Space
- Total Swap Space

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

- Connections Available
- Connections in Use
- Maximum Connections Used
- Total Connections
- Maximum Connections Allowed

The **Site Associations** tab contains the following information:

- Site Associations Recompute in Progress
- Site Queue Length
- Last Recompute Started
- Last Recompute Completed

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

- Collections Requested in Last 5 minutes
- Collections Completed in Last 5 minutes
- Collections in Process
- Time to Execute Skips in Last 5 minutes
- Collection Collector State Count in Last 5 minutes

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

Glossary

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.

F

forwardable filters

The QA probes that are excluded and are not forwarded to the global manager based on the discovery filter

H

High

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

I

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

Local QA Probes

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

Local Sites

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

Low

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

M

Mean Opinion Score (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

Some examples of network elements are routers, switches, and phone connections

network elements

Some examples of network elements are routers, switches, and phone connections

Nominal

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

Not Polled

Indicates that this network element is not polled intentionally.

O

ODBID

ODBID is a custom attribute that the NNMi topology uses to integrate the NNMi topology with Business Service Management(BSM) software suite. The NNM iSPIs get this attribute from NNMi during the discovery and keep a reference. You can use ODBID as a report toplogy filter.

P

Packet Loss

Packet loss occurs when one or more transmitted packets fail to reach their destination. This metric is measured in percentage.

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

Remote QA Probes

Remote QA probes are primarily discovered and polled at the regional manager.

Remote Sites

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

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

site rules

Configuration associated to a site are called site rules. For example Node Group, Ordering, Test Name Pattern, etc are the site rules that are used to configure a site. The rules are prioritized inherently. The Node Group rule has the highest priority, the IP Address rule the second highest priority. Test Name Pattern rule has the third highest priority while the VRF Name rule has the the lowest priority among these four rules. Note that none of these rules have any dependency to each other. In other words, while creating a site, you can specify all or any of the the rules.

sites

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

standard deviation

Standard deviation is a measurement of variability used in statistics and probability theory. It shows how much variation is there from the average or mean value. A low standard deviation indicates the values tend to be close to the average mean value whereas a high standard deviation indicates the data is spread out over a wide range of values.

standard IPv6 shorthand notation

IPv6 addresses are generally written in the form,

hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hh-hh. 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.

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.

We appreciate your feedback!

If an email client is configured on this system, click Send Email

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

Product name and version:

Document title:

Feedback:


Java™
COMPATIBLE