

HP Network Node Manager iSPI Performance for Traffic Software

For the Windows® and Linux operating systems

Software Version: 9.20 (Patch 1)

[Online Help](#)

Document Release Date: November 2012

Software Release Date: October 2012



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.

Copyright Notice

© Copyright 2009 - 2012 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

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

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

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

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

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>)

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

Online Help.....	1
Oracle Technology — Notice of Restricted Rights.....	2
Contents.....	6
HP Network Node Manager iSPI Performance for Traffic Software.....	10
Configuring the NNM iSPI Performance for Traffic.....	12
Configuring Leaf Collector Systems.....	13
Add Leaf Collector Systems.....	14
Edit Leaf Collector Systems.....	15
Delete Leaf Collector Systems.....	15
Configuring Leaf Collector Instances.....	15
Add a Leaf Collector Instance.....	16
Editing a Leaf Collector Instance.....	18
Deleting a Leaf Collector Instance.....	19
Starting and Stopping a Leaf Collector Instance.....	20
Configuring Master Collectors.....	20
Configure Flow Forwarders.....	22
Edit Flow Forwarders.....	23
Start and Stop Flow Forwarders.....	23
Delete Flow Forwarders.....	24
Flow Exporters.....	24
Flow Exporter History.....	24
Configure Sites.....	24
Site Priority.....	25
Guidelines for Defining a Site.....	25
Add Sites.....	25
Edit Sites.....	26
Delete Sites.....	28
Configure Filters.....	28

Add Filters.....	28
Edit Filters.....	29
Delete Filters.....	30
Filter Groups.....	30
Add a New Filter Group.....	31
Edit a Filter Group.....	31
Delete a Filter Group.....	31
Application Mapping.....	32
Define a New Application.....	32
Edit an Application Mapping Definition.....	33
Delete an Application.....	34
Application Mapping Groups.....	35
Add a New Application Mapping Group.....	35
Edit an Application Mapping Group.....	36
Delete an Application Mapping Group.....	36
Creating Filter Groups and Application Maps from the Command Line.....	36
Configure Classes of Service.....	38
Add Class of Service Definitions.....	38
Edit Class of Service Definitions.....	38
Delete TOS Groups.....	39
Top N Application Inclusion List.....	39
Configuring Threshold to Monitor Traffic Flow.....	40
Launching the Threshold Configuration Panel.....	40
Adding New Threshold Settings Using the Threshold Details Form.....	41
Adding New Threshold Settings for Interfaces Using the Traffic Analysis Workspace.....	44
Adding New Threshold Settings for Nodes Using the Traffic Analysis Workspace.....	48
Adding New Threshold Settings for Sites Using the Traffic Analysis Workspace.....	50
Modifying Threshold Settings Using the Threshold Details Form.....	53
Deleting Threshold Settings Using the Threshold Details Form.....	53
Diagnosing the Health of the NNM iSPI Performance for Traffic.....	56
Verifying the Installation Configuration Parameters for Master Collector.....	56

Viewing Unresolved IPs.....	59
Listing the Undefined Applications for a Leaf Collector.....	60
Threshold Exceptions Reporting Nodes View.....	60
Analysis Pane in the Threshold Breached Reporting Nodes view.....	60
Threshold Exceptions Reporting Interfaces View.....	61
Analysis Pane in the Threshold Breached Reporting Interfaces view.....	61
Incident Types Supported by NNM iSPI Performance for Traffic.....	62
NNM iSPI Performance for Traffic Maps.....	64
Accessing Maps.....	64
Types of Maps.....	64
Global Network Management Environment.....	66
Add Remote Leaf Collectors.....	66
Edit Remote Leaf Collectors.....	67
Add Remote Master Collectors.....	67
Edit Remote Master Collectors.....	68
Accessing Details of Traffic Data Sources.....	70
Traffic Reporting Interfaces View.....	70
Analysis Pane in the Traffic Reporting Interfaces view.....	70
Traffic Reporting Interface Form.....	72
Traffic Reporting Nodes View.....	74
Analysis Pane in the Traffic Reporting Nodes view.....	74
Traffic Node Form.....	76
Disabling Interfaces to Report Flow Data.....	76
NNM iSPI Performance for Traffic Leaf Collectors.....	77
Viewing Collector Statistics History.....	78
Viewing Flow Processing Status.....	78
Site Inventory Analysis Using the Traffic Sites View.....	79
Analysis Pane in the Traffic Reporting Interfaces view.....	79
Traffic Site Form.....	80
Storing and Analyzing Flow Packets.....	82
Analyze Flow Packets.....	83
Contents of the Flow Packet Files.....	85

Limiting the Number of the Flow Packet Files..... 85

Chapter 1

HP Network Node Manager iSPI Performance for Traffic Software

The HP Network Node Manager iSPI Performance for Traffic Software (NNM iSPI Performance for Traffic) extends the capability of HP Network Node Manager i Software (NNMi) to monitor the performance of the network.

The NNM iSPI Performance for Traffic enriches the obtained data from the IP flow records that are exported by the routers in your NNMi network.

The NNM iSPI Performance for Traffic aggregates the IP flow records, correlates the IP flow records with the NNMi topology, and enables you to generate performance reports by exporting data to the Network Performance Server (NPS). It also enables you to configure deployment-specific enrichment attributes like site and applications and provides traffic-related information in the form of inventory views and maps in the NNMi console.

Chapter 2

Configuring the NNM iSPI Performance for Traffic

The NNM iSPI Performance for Traffic Configuration form enables you to configure different elements required for creating the network traffic monitoring environment. You can configure the [Leaf Collectors](#)¹ and [Master Collector](#)² to receive the traffic data from different devices. You can create filters to filter out the unnecessary information and retain only the data that you are interested in.

Note: To use the Configuration form, you must log on to the NNMi console as an administrator.

To log on to the NNM iSPI Performance for Traffic Configuration form:

1. Log on to the NNMi console with the administrator privileges.
2. Go to the Configuration workspace.
3. Double-click **NNM iSPI Performance for Traffic Configuration**. The NNM iSPI Performance for Traffic form opens.
4. Log on to the NNM iSPI Performance for Traffic form with the `system` user account created during the installation of the Master Collector.

The following table lists the configuration tasks.

Configure the NNM iSPI Performance for Traffic

What You Can Configure	Description
Leaf Collectors	Using the Leaf Collector Systems view, you can add the details of Leaf Collector systems.
Master Collectors	Using the Master Collector Systems view, you can add the details of Master Collector systems.
Flow Forwarders	Using the Flow Forwarder view, you can add the details of Flow Forwarders associated with Leaf Collectors.
Filters	Using the Filters view, you can create filters to filter out unwanted data and retain only the information that is relevant to you.

¹The Leaf Collector receives flow packets from different flow-enabled devices and summarizes the data into flow records.

²The Master Collector receives the processed IP flow from the Leaf Collectors and exports the data to the NPS to generate performance reports.

What You Can Configure	Description
Application Mapping	Using the Application Mapping view, you can associate different flow attributes with different applications running on your network.
Sites	Using the Sites view, you can define sites in your environment. With this configuration, you can generate traffic reports with the data obtained from specific sites.
Type of Service Groups	Using the Type of Service Groups view, you can group flow packets based on the Type of Service (ToS) values.

After installing the NNM iSPI Performance for Traffic, follow these steps:

1. Configure Leaf Collector systems.
2. Configure Leaf Collector instances.
3. Configure the Master Collector.
4. Configure additional properties:
 - a. Configure sites.
 - b. Configure filters.
 - c. Define a new application.
 - d. Configure Classes of Service.
5. Associate all the additional properties with the Leaf Collector instance.

Configuring Leaf Collector Systems

The NNM iSPI Performance for Traffic Configuration form enables you to configure multiple Leaf Collector instances that you want to deploy on the network. You can start and configure multiple Leaf Collector instances on a single system. Therefore, before configuring individual leaf Collector instances, it is important to add the Leaf Collector systems first in the NNM iSPI Performance for Traffic Configuration form.




The Leaf Collector Systems view displays all the configured Leaf Collector systems on the network (systems where you installed the Leaf Collector). You can open an existing Leaf Collector System to view the details of the configuration. You can modify the properties of the Leaf Collector system with the help of this view.

To display the Leaf Collector Systems view, go to the NNM iSPI Performance for Traffic Configuration form, and then click **Leaf Collector Systems**. The Leaf Collector Systems view opens.

The following table lists different uses of the view.

Uses of the Leaf Collector Systems View

Use	Description
Add a new Leaf Collector system	Open a new form to add a new Leaf Collector system by

Use	Description
	clicking the Add  button.
View the details of existing Leaf Collector systems	The view presents the details of all the Leaf Collector systems that are already added.
Edit the properties of existing Leaf Collector systems	Open a new form by clicking the Open  button to edit the properties (like hostname, password, or port) of a system that was already added.
Delete a Leaf Collector system that was configured with the monitoring solution	Open a new form to delete an existing Leaf Collector from the list of configured Leaf Collector systems by clicking the Open  button.


The basic attributes of the Leaf Collector System view are the following:

Attribute	Description
Hostname	The fully qualified domain name of the Leaf Collector system.
HTTP Port	The HTTP port number of the Leaf Collector system.
JNDI Port	The JNDI port number of the Leaf Collector system.
Leaf Count	Number of Leaf Collector instances running on the system.

Add Leaf Collector Systems

You must configure the NNM iSPI Performance for Traffic by adding Leaf Collector instances in the Leaf Collector view. You cannot use the data provided by Leaf Collectors unless you add the Leaf Collector instances and Leaf Collector systems to the NNM iSPI Performance for Traffic views.

To add a Leaf Collector system:


1. In the NNM iSPI Performance for Traffic Configuration form, click **Leaf Collector Systems**.
2. Click the  Add icon. A new form opens.
3. In the form, specify necessary details in the following fields:
 - Container Hostname: Type the fully-qualified domain name of the Leaf Collector system.
 - Password: Type the password of the `system` account on the Leaf Collector system (this is the password that you specified during the installation of the Leaf Collector).
 - JNDI Port: Type 11099; this is the JNDI port number of the Leaf Collector system (you cannot change this value).
 - HTTP Port: Type 11080; this is the HTTP port number of the Leaf Collector system (you cannot change this value).
4. Click **Save & Close**.

Edit Leaf Collector Systems

The Leaf Collector Systems view enables you to change the properties of existing Leaf Collector systems that have already been added to the view. You must edit the properties of a Leaf Collector system if you change one or all of the following properties of the system:

- The administrative or root password of the system
- JNDI port
- HTTP port


To edit the properties of a Leaf Collector system:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Leaf Collector Systems**.
2. Select the Leaf Collector system that you want to edit.
3. Click the  Open icon. A new form opens. The form presents two sections:
 - Collector System Details: This section enables you to modify the properties of the system.
 - Leaf Collectors on this System: This section presents the details of all the Leaf Collectors that are running on the system.
4. In the Collector System Details section, modify the values in the following fields:
 - Leaf Password
 - JNDI Port
 - HTTP Port
5. Click **Save & Close**.

Delete Leaf Collector Systems

Before you remove a specific Leaf Collector System from the environment, you must use the Leaf Collector view to delete the Leaf Collector instances configured for that system.

To remove a Leaf Collector system from the view:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Leaf Collector Systems**.
2. Select the Leaf Collector system that you want to edit.
3. Click the  Delete icon.

Configuring Leaf Collector Instances

The NNM iSPI Performance for Traffic Configuration form enables you to configure individual Leaf Collector instances that you want to deploy on the network. You can create and configure multiple Leaf Collector instances on a single system.




Before configuring multiple Leaf Collector instances to run on a single system, make sure that you have sufficient resources on the system.

The Leaf Collectors view provides you with an interface to add and modify collector instances to the view. You can delete an existing collector instance from the Leaf Collectors view. The view also displays all the configured Leaf Collector instances on the network and helps you start or stop the collector instances of your choice.

To display the Leaf Collectors view, go to the NNM iSPI Performance for Traffic Configuration form, click **Leaf Collectors**. The Leaf Collectors view opens.

The following table lists different uses of the view.

Uses of the Leaf Collectors View

Use	Description
Add a new Leaf Collector instance	Open a new form to add a new Leaf Collector instance by clicking the Add  button.
View the details of existing Leaf Collector instances	The view presents the details of all the Leaf Collector instances that are already added.
Edit the properties of existing Leaf Collector instances	Open a new form by clicking the Open  button to edit the properties of a collector instance that was already added.
Delete a Leaf Collector instance that was configured with the monitoring solution	Open a new form to delete an existing Leaf Collector instance from the list of configured Leaf Collector instances by clicking the Open  button.

The following table lists the basic attributes of the Leaf Collectors view:


Leaf Collector Attributes

Attribute	Description
Collector Name	The name of the Leaf Collector instance.
Status	The status of the Leaf Collector system.
IP	The IP address of the Leaf Collector system.
Collector Type	The type of Leaf Collector instance running on the system. Possible values are: <ul style="list-style-type: none"> • Netflow • Sflow • JFlow • IPFIX
Container Hostname	The Fully qualified domain name of the system that hosts the collector instance.
Listen Port	The Port where the collector instance listens for incoming traffic packets.

Add a Leaf Collector Instance

You must configure the NNM iSPI Performance for Traffic by adding Leaf Collector instances in the Leaf Collector view.

To add a leaf collector instance:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Leaf Collectors**.
2. Click the  **Add** icon. A new form opens. The form presents the following two different sections:
 - Leaf Collector Details: You must specify necessary details of the collector here.
 - The other section presents multiple tabs to display additional properties associated with the collector.
3. In the Leaf Collector Details section, specify the values in the following fields:
 - Collector Type: Select the any of the following collector types:
 - netflow: ¹
 - ipfix: ²
 - sflow: ³
 - Listen Port: Specify the port where the collector listens for incoming flow packets (must be in the range of 1024-65535).
 - IP: Type the IP address of the Leaf Collector system.
 - Store Flow in File: Select **true** if you want to store the incoming flow packets in a file on the Leaf Collector system.

Use this feature only for troubleshooting. This option has a significant impact the performance of the Leaf Collector.

If you select true, the flow packet files are created in the following directory on the Leaf Collector system:

On Windows:
 <Data_Dir>\shared\traffic-leaf\data\<Leaf_Collector_Instance>\<IP_Address_of_Source>

On Linux:
 /var/opt/OV/shared/traffic-leaf/data/<Leaf_Collector_Instance>/<IP_Address_of_Source>

In this instance:
 <Data_Dir>: Data directory that you chose during the installation of the Leaf Collector.
 <Leaf_Collector_Instance>: Name of the Leaf Collector instance
 <IP_Address_of_Source>: IP address of the device where the flow packet originated.

 - Source IP DNS Lookup: Set this to **true** if you want to enable DNS lookup of the source of the flow packet.
 - Destination IP DNS Lookup: Set this to **true** if you want to enable DNS lookup of the destination of the flow packet.
4. *Optional.* Add secondary properties of the collector in the other section:
 - In the Filter Groups tab, associate a filter group with the Leaf Collector.
 - In the All TOS Groups, tab, associate a TOS group with the Leaf Collector.

¹Select this option, if you want the new leaf collector to process NetFlow traffic.

²Select this option, if you want the new leaf collector to process IPFIX traffic.


³Select this option, if you want the new leaf collector to process sFlow traffic.

5. In the All Application Mapping Groups tab, associate an application mapping group with the Leaf Collector. If you have not created any application mapping groups, you *must* select the `DefaultAppMapGroup` to be able to sort and rank metrics by applications on reports.
6. In the All Leaf Collector Systems tab, select the hostname of the system where you installed the Leaf Collector.
7. Click **Save & Close**.

Editing a Leaf Collector Instance

At any point during operation, you can change the properties of collector instances that you provided to your NNM iSPI Performance for Traffic deployment. You can use the Leaf Collectors view to edit the details of existing Leaf Collector instances.

To edit the properties of a Leaf Collector instance:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Leaf Collectors**.
2. Select the Leaf Collector instance that you want to edit.
3. Click the  Open icon. A new form opens. The form presents the following two different sections:
 - Leaf Collector Details: Lists the details of the collector.
 - The other section presents multiple tabs to display additional properties associated with the collector.
4. The Leaf Collector Details section displays the following primary properties of the collector.
 - Collector Type: Select the any of the following collector types:
 - netflow: ¹
 - ipfix: ²
 - sflow: ³
 - Listen Port: Specify the port where the collector listens for incoming flow packets (must be in the range of 1024-65535).
 - IP: Displays the IP address of the Leaf Collector system. You cannot modify the value in this field.
 - Store Flow in File: Select **true** if you want to store the incoming flow packets in a file on the Leaf Collector system.

Note: Use this feature only for troubleshooting. This option has a significant impact the performance of the Leaf Collector.

¹Select this option, if you want the new leaf collector to process NetFlow traffic.

²Select this option, if you want the new leaf collector to process IPFIX traffic.

³Select this option, if you want the new leaf collector to process sFlow traffic.

If you select true, the flow packet files are created in the following directory on the Leaf Collector system:

On Windows:

`<Data_Dir>\shared\traffic-leaf\data\<Leaf_Collector_Instance>\<IP_Address_of_Source>`

On Linux:


`/var/opt/OV/shared/traffic-leaf/data/<Leaf_Collector_Instance>/<IP_Address_of_Source>`

- Source IP DNS Lookup: Set this to **true** if you want to enable DNS lookup of the source of the flow packet.
 - Destination IP DNS Lookup: Set this to **true** if you want to enable DNS lookup of the destination of the flow packet.
5. Modify the secondary properties of the collector. The other pane on this form enables you to view and modify the association of the collector with existing filters, applications, and ToS groups.
- Applied Filter groups: In the Filter Groups tab, select a filter group that you want to apply on the collector or deselect a filter group that you want to dissociate from the collector.
 - Applied Application Mapping groups: In the Applied Application Mapping Groups tab, select an application group that you want to apply on the collector or deselect an application group that you want to dissociate from the collector.
 - ToS groups: In the TOS Groups tab, select a ToS group that you want to apply on the collector or deselect a ToS group that you want to dissociate from the collector.
 - Flow Forwarding Destinations: In the Flow Forwarding Destinations tab, select a Flow Forwarder that you want to associate with the collector or deselect a Flow Forwarder that you want to dissociate from the collector.
 - Flow Exporters: In the Flow Exporters tab, select a Flow Exporter that you want to associate with the collector or deselect a Flow Exporter that you want to dissociate from the collector.
 - Collector Statistics History: Displays the last 11 flush entries that the leaf collector has processed and flushed to the master collector.
 - Collector Health: Displays the health of the leaf collector. This tab lists the following information:
 - All the problems that the selected leaf collector encountered during its operation. The Start Time and End Time columns display the time when the problem started and got resolved.
 - Suggestions to resolve the problems
 - Status of the problems
6. Click **Save & Close**.

Deleting a Leaf Collector Instance


Before you remove the Leaf Collector from your environment, you must delete the Leaf Collector instance from the Leaf Collectors view.

To delete a Leaf Collector instance:


1. In the NNM iSPI Performance for Traffic Configuration form, click **Leaf Collectors**.
2. Select the Leaf Collector instance that you want to delete.
3. Click the  Delete icon.

Starting and Stopping a Leaf Collector Instance

To start a Leaf Collector instance:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Leaf Collectors**.
2. Select the Leaf Collector instance that you want to start.
3. Click the  **Start** icon.

To stop a Leaf Collector instance:

1. Go to the Leaf Collectors view.
2. Select the Leaf Collector instance that you want to stop.
3. Click the  **Stop** icon.

Configuring Master Collectors

After adding all the details of Leaf Collectors in the NNM iSPI Performance for Traffic Configuration form, you must set up the Master Collector in your environment, which includes adding details like the hostname of the Master Collector system and the flush record limit of collector in the NNM iSPI Performance for Traffic Configuration form.

You must set up only one Master Collector in your environment. However, in a GNM setup, you can add a Master Collector that belongs to a different regional manager to your region.

To set up the Master Collector:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Master Collectors**.
2. In the Master Collector form, click  **Edit** to update any of the following fields:

Attribute	Description
Master Hostname	Indicates the hostname of the master collector. Type the FQDN of the Master Collector system
Source IP DNS Lookup	Indicates whether the NNM iSPI Performance for Traffic

Attribute	Description
	<p>should perform IP DNS lookup at the source or not. Possible values are :</p> <ul style="list-style-type: none"> ■ True ■ False <p>Set this to true if you want to enable DNS lookup of the source of a flow packet.</p> <p>Do not set this field to true if you already configured DNS lookup for sources for Leaf Collectors.</p>
Destination IP DNS Lookup	<p>Indicates whether the NNM iSPI Performance for Traffic should perform IP DNS lookup at the destination or not. Possible values are :</p> <ul style="list-style-type: none"> ■ True ■ False <p>Set this to true if you want to enable DNS lookup of the destination of a flow packet.</p> <p>Do not set this field to true if you already configured DNS lookup for destinations for Leaf Collectors.</p>
Flush Record Limit	<p>Indicates the record limit for the Master Collector to flush the IP flow data records to the NPS database.</p> <p>Once the number of records in the Master Collector reaches the limit specified in this field, the Master Collector flushes the records to NPS.</p>
DNS Lookup Type	<p>Indicates whether the NNM iSPI Performance for Traffic should find the IP address of the specified domain name in a case sensitive manner or not. Possible values are:</p> <ul style="list-style-type: none"> ■ As-Is¹ ■ Uppercase² ■ Lowercase³
Interface Traffic Data Flush	<p>Indicates whether the Leaf Collector should flush the Interface Traffic data.</p>

¹ NNM iSPI Performance for Traffic finds the IP address for the specified domain name without converting the case of the domain name

² NNM iSPI Performance for Traffic finds the IP address for the specified domain name after converting the domain name in uppercase.

³ NNM iSPI Performance for Traffic finds the IP address of the specified domain name after converting the domain name in lowercase.


Attribute	Description
	<p>Possible values are:</p> <ul style="list-style-type: none"> ■ Disable Flush: If you select this value, the Leaf Collector does not flush Interface Traffic data to the Master Collector and the Master Collector stops generating the data for the extension pack Interface_Traffic. ■ Enable Flush: If you select this value, the Leaf Collector flushes Interface Traffic data to the Master Collector and the Master Collector generates the data for the extension pack Interface_Traffic.
nms.traffic-master.maxflowrecord.inqueue	Indicates the maximum number of flow records that the Master Collector can queue while accepting the input from the Leaf Collectors.
com.hp.ov.nms.spi.traffic-master.spi.jndi.port	Indicates the JNDI port that the Master Collector uses.
com.hp.ov.nms.spi.traffic-master.spi.secureport	Indicates the port the Master Collector uses for HTTPS communication.
com.hp.ov.nms.spi.traffic-master.spi.port	Indicates the port the Master Collector uses for HTTP communication
com.hp.ov.nms.spi.traffic-master.spi.isSecure	Indicates whether the Master Collector uses secure mode of communication (HTTPS) to communicate with the NNMI server

3. Click  **Save**.

Configure Flow Forwarders

Flow Forwarders are configured on a Leaf Collector; this configuration enables forwarding of IP flow records to a specified location. The destination where the flow data needs to be sent is identified with the IP address and port number combination. You can configure multiple flow forwarding destinations for each Leaf Collector instance.

To add a Flow Forwarder:


1. In the NNM iSPI Performance for Traffic Configuration form, click **Flow Forwarders**.
2. In the Flow Forwarders view, click the  Add icon. A new form opens with the following sections:
 - **Flow Forwarder Details:** In this section, you must specify the primary details of the Flow Forwarder you want to add.
 - The other section lists the available Leaf Collectors in the environment. You can use the check boxes () to associate Leaf Collectors to the Flow Forwarder.

3. In the Flow Forwarder Details section, specify the following details:
 - Flow Forwarder Name: Type the name of the Flow Forwarder.
 - Forwarding IP: Type the IP address of the Flow Forwarding system.
 - Forwarding Port: Type the port number of the Flow Forwarding system.
4. In the other section, select checkboxes () to associate Leaf Collectors to the Flow Forwarder. You can link multiple Leaf Collectors with a Flow Forwarder.
5. Click **Save**.

Edit Flow Forwarders

The Flow Forwarders view in the NNM iSPI Performance for Traffic Configuration form presents you the list of configured Flow Forwarders. You can edit the properties of the existing Flow Forwarders from this view.


To edit a Flow Forwarder:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Flow Forwarders**.
2. In the Flow Forwarders view, select a Flow Forwarder that you want to edit.
3. Click the  Open icon. A new form opens with the following sections:
 - Flow Forwarder Details: In this section, you can modify the primary details of the Flow Forwarder you want to edit.
 - The other section lists the available Leaf Collectors in the environment. You can use the check boxes () to modify the relationship of a Flow Forwarder with Leaf Collectors.
4. In the Flow Forwarder Details section, modify the following details if required:
 - Flow Forwarder Name: The name of the Flow Forwarder.
 - Forwarding IP: The IP address of the Flow Forwarding system.
 - Forwarding Port: The port number of the Flow Forwarding system.
5. In the other section, select checkboxes () to associate Leaf Collectors to the Flow Forwarder or clear checkboxes () to dissociate Leaf Collectors from the Flow Forwarder. You can link multiple Leaf Collectors with a Flow Forwarder.
6. Click **Save**.

Start and Stop Flow Forwarders

After adding a new Flow Forwarder or modifying an existing Flow Forwarder, you must start it.

To start a Flow Forwarder:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Flow Forwarders**.
2. In the Flow Forwarders view, select a Flow Forwarder that you want to start.
3. Click the  Start icon. The Flow Forwarder starts operating.

To stop a Flow Forwarder:


1. In the NNM iSPI Performance for Traffic Configuration form, click **Flow Forwarders**.
2. In the Flow Forwarders view, select a Flow Forwarder that you want to stop.

3. Click the  Stop icon. The Flow Forwarder stops operating.

Delete Flow Forwarders

You can delete Flow Forwarders from the Flow Forwarders view in the NNM iSPI Performance for Traffic Configuration form.

To delete a Flow Forwarder:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Flow Forwarders**.
2. In the Flow Forwarders view, select a Flow Forwarder that you want to edit.
3. Click the  Delete icon.

Flow Exporters

Flow Exporters are the nodes or devices on the network that host the flow collector interfaces. With every Leaf Collector instance, you must associate a flow collector interface that is capable of sending the traffic flow information. When you configure a Leaf Collector instance, you must specify the Flow Exporter details (see "[Add a Leaf Collector Instance](#)" (on page 16)). The Flow Exporters view provides you with a list of available devices that send traffic flow information to Leaf Collectors.

Flow Exporter History

You can view a record of all the exchanges done by a Flow Exporter. You can launch a new view from the Flow Exporter view, which presents the historical data. This view presents the following details in a tabular fashion where each row represents a flush:

- IP: The IP address of the Flow Exporter.
- Flush time: Date and time when the Flow Exporter flushed data to the Leaf Collector.

Tip: Click the  Refresh icon to retrieve the details of the most recent flush.

- Number of flows: The number of flow packets transmitted to the Leaf Collector with the flush.

To view the Flow Exporter history:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Flow Exporters**.

The Flow Exporters view opens. The view lists all the available devices on the network that send traffic flow information to Leaf Collectors.

2. In the Flow Exporters view, select a Flow Exporter, and then click  **Open**.

Configure Sites

The NNM iSPI Performance for Traffic Configuration form enables you to define sites in your networking environment. You can view traffic reports for specific sites to identify site-specific performance bottlenecks in your organization's network infrastructure.

When a flow collector sends a flow packet to the Leaf Collector, the source and destination sites of the flow packet are computed by the Leaf Collector based on the sites that you configure with the help of the NNM iSPI Performance for Traffic Configuration form.

You can define a site by a specific IP address or a range of IP addresses. The NNM iSPI Performance for Traffic associates the flow with a site if the origin or destination of the flow is a system whose IP address that defines the site. You can also use the wildcard character (*) in the IP address while defining a site. Before you use the NNM iSPI Performance for Traffic Configuration form to define sites, see ["Guidelines for Defining a Site" \(on page 25\)](#).

Site Priority

By defining the site priority, you configure the Leaf Collector to process site information of received flow packets in a specific order. The Leaf Collector prioritizes processing of flow packets associated with high priority sites.

Guidelines for Defining a Site

Follow these guidelines when you define sites in the NNM iSPI Performance for Traffic Configuration form by specifying IP address:

- You can use an IP address, an IP address range, or an IP address with the wildcard character (*) to define a site.
- You can use the wildcard character in one or more (or all) octets of the IP address while defining the site.


When you use wildcards for all four octets while defining the site, the NNM iSPI Performance for Traffic associates the site to all flow packets collected from the network. If the IP address pattern matches the SrcIP of the flow it will map it to a Source Site Name field.

- You can use an IP address range instead of a single IP address for defining a site. You can use ranges in one or more (or all) octets of the IP address while defining the site. For example, 179.16.2-20.1-100.

Add Sites

Although it is optional to add site definitions in the NNM iSPI Performance for Traffic Configuration form, you can enrich traffic reports with the option to group data by sites.

To add a new site:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Sites**.
2. In the Sites view, click  **Add**. A new form opens with the following sections:
 - Site Details: In this section, you must specify the primary details of the site you want to add.
 - The other section displays the list of similar sites that exist in the environment.
3. In the Site Details section, specify the following details:
 - Site Name: Type the name of the Site. Do not use any special characters other than the hyphen (-) and underscore (_).
 - Tenant: Select an NNMi tenant from the list of tenants created in NNMi.

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

You can select the following options based on the selected tenant:

- Sites with higher, lower, or equal priority
- Sites in the same IP range
- *Optional.* Site Description: Type a description of the site.
- *Optional.* Site Priority: Type the priority of the site (an integer between 0 and 65535). The NNM iSPI Performance for Traffic considers that the value 0 is of the highest priority and the value 65535 is of the lowest priority.

To view the sites of higher priority, click **Show Higher Priority Sites**. The Higher Priority Sites tab displays existing sites that have a higher priority assigned to them.

To view the sites of lower priority, click **Show Lower Priority Sites**. The Lower Priority Sites tab displays existing sites that have a lower priority assigned to them.

To view the sites with the equal priority value, click **Show Same Priority Sites**. The Same Priority Sites tab displays existing sites that have the same priority assigned to them.

NNM iSPI Performance for Traffic displays the sites with higher, lower, or equal priority for the selected tenant.

- Site IP Configuration: In this section, type the following detail:
New IP/Range: Type the IP address or range of IP addresses to define the site. You can use the wildcard character (*) while specifying the IP address. For guidelines on specifying this parameter, see ["Guidelines for Defining a Site" \(on page 25\)](#).
If the SrcIP or DstIP attribute (or both) of a packet matches the IP address (or the IP address range) specified in this field, the NNM iSPI Performance for Traffic associates the packet to the site.
For example, if you specify 172.16.*.*, flow packets with 172.16.2.1 as the SrcIP or DstIP attribute are associated to the site.

After typing the value, click **Add**.

To include more IP address (or IP address ranges) in the site definition, type the address or range in the New/IP Range box, and then click **Add**.

If you specify an IP address range, click **Show Sites in the Same IP Range** to view the sites that are in the same IP range. The Sites in the Same IP Range tab displays sites that are in the same IP range.


NNM iSPI Performance for Traffic displays the sites within the same IP range for the selected tenant.

4. Click **Save & New** to create another site or **Save & Close** to close the form.

Edit Sites

You can modify definitions [Edit Sites](#) of the existing sites.

To modify a site:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Sites**.
2. In the Sites view, select a site, and then click  **Open**. A new form opens with the following sections:
 - **Site Details:** In this section, you can modify the primary details of the site that you selected.
 - The other section lists similar sites that exist in the environment.
3. In the Site Details section, you can modify the following details:
 - **Site Name:** The name of the Site. Do not use any special characters other than the hyphen (-) and underscore (_).
 - **Tenant:** Select an NNMi tenant from the list of tenants created in NNMi.

NNMi provides a tenant named Default Tenant and assigns each newly discovered node to the Default Tenant and the Security Group attribute value configured for the Default Tenant. As an NNMi administrator, you can create new tenants and security groups. See *Configure Tenants* and *Configuring Security* in *HP Network Node Manager i Software Online Help: Help for Administrators*.
 - **Site Description:** The description of the site.
 - **Site Priority:** The priority of the site (an integer between 0 and 65535). The NNM iSPI Performance for Traffic considers that the value 0 is of the highest priority and the value 65535 is of the lowest priority.

To view the sites of higher priority, click **Show Higher Priority Sites**. The Higher Priority Sites tab displays existing sites that have a higher priority assigned to them.

To view the sites of lower priority, click **Show Lower Priority Sites**. The Lower Priority Sites tab displays existing sites that have a lower priority assigned to them.

To view the sites with the equal priority value, click **Show Same Priority Sites**. The Same Priority Sites tab displays existing sites that have the same priority assigned to them.
 - **Site IP Configuration:** In this section, you can modify the following detail:
 - **New IP/Range:** The IP address or range of IP addresses to define the site. You can use the wildcard character (*) while specifying the IP address. For guidelines on specifying this parameter, see ["Guidelines for Defining a Site" \(on page 25\)](#).

If the `SrcIP` or `DstIP` attribute (or both) of a packet matches the IP address (or the IP address range) specified in this field, the NNM iSPI Performance for Traffic associates the packet to the site.

For example, if you specify `172.16.*.*`, flow packets with `172.16.2.1` as the `SrcIP` or `DstIP` attribute are associated to the site.

After typing the value, click **Add**.

To include more IP address (or IP address ranges) in the site definition, type the address or range in the New/IP Range box, and then click **Add**.

If you specify an IP address range, click to view the sites that are in the same IP range. The Sites in the Same IP Range tab displays sites that are in the same IP range.


While editing a site, the tabs in the right pane continue to display the site with its old properties. For example, if you change the priority of a site from 2 to 3, and then if you click

Higher Priority Sites tab, the same site is displayed there with the priority 2. Changes do not completely take effect until you click **Save & Close**.

4. Click **Save & Close**.

Delete Sites

To delete a site:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Sites**.
2. In the Sites view, select a site, and then click the  **Delete**.
3. In the confirmation dialog box, click **Delete**.

Configure Filters

Filters enable to filter out flow packets that are not of your interest. The NNM iSPI Performance for Traffic Configuration form enables you to define filters to utilize only the relevant flow packets for traffic flow monitoring. The filtering mechanism of the NNM iSPI Performance for Traffic enables you to either **drop** or **keep** flow packets based on the filter definitions that you create.

You can create filtering conditions using the following attributes of a flow packet:


- ProducerIP: IP address of the system where the flow collector is located.
- SrcIP: IP address of the system where the traffic flow originated.
- DstIP: IP address of the system where the traffic flow terminated.
- IPProtocol: Protocol used by the traffic flow.
- NFSNMPInputIndex: SNMP index of the egress interface
- NFSNMPOutputIndex: SNMP index of the ingress interface
- DstPort: Ingress port
- TCPFlags: TCP flag of the traffic flow
- IPToS: Type of Service property of the traffic flow

The NNM iSPI Performance for Traffic enables you to define a filter with multiple conditions by assigning the AND operator on the conditions.

Add Filters

The NNM iSPI Performance for Traffic Configuration form enables you to add filter conditions to filter out unnecessary flow packets. Although optional, creating filters simplifies the process of analyzing the traffic flow packets by discarding irrelevant and unnecessary flow packets.

To add a new filter:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Filters**.
2. In the Filters view, click the  Add icon. A new form opens with the following sections:
 - Filter Details: In this section, you must specify the primary details of the filter you want to add.
 - The other section lists related details.
3. In the Filter Details section, select the filter operation.

If you select **keep**, the NNM iSPI Performance for Traffic retains only the packets that satisfy the condition of the filter and discards all other packets.

If you select **drop**, the NNM iSPI Performance for Traffic discards only the packets that satisfy the condition of the filter and retains all other packets.
4. You can create new conditions and delete or modify the existing conditions.

To create a new condition:


 - a. Select an attribute.
 - b. Select an operator. For the ProducerIP, SrcIP, and DstIP attributes, you can choose the like, equals, or not-equals operator. For the other attributes, you can choose the =, !=, <=, or >= operator.

The Filter Text Configuration tab in the right pane shows the condition that you define in the Filter Details section. The All Filter Groups tab shows the list of all defined filter groups.
 - c. Specify the value to be compared.
 - d. Click **Add**. Another row of attributes and operators appears.
 - e. To add another condition, repeat the above steps. If you define multiple conditions, the NNM iSPI Performance for Traffic assigns the AND operator on them while performing the filtering action.
 - f. *Optional*. If filter groups are already defined, you can associate the filter with a filter group from the All Filter Groups tab. By default, the NNM iSPI Performance for Traffic places the new filter in DefaultFilterGroup.
5. Click **Save & Close**.

Edit Filters

You can use the NNM iSPI Performance for Traffic Configuration form to edit existing filters.

To edit a filter:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Filters**.
2. In the Filters view, select the filter that you want to modify, and then click the  Open icon. A new form opens with the following sections:
 - Filter Details: In this section, you can modify the primary details of the filter you want to add.
 - The other section lists related details.
3. In the Filter Details section, select the filter operation.

If you select **keep**, the NNM iSPI Performance for Traffic retains only the packets that satisfy the condition of the filter and discards all other packets.

If you select **drop**, the NNM iSPI Performance for Traffic discards only the packets that satisfy the condition of the filter and retains all other packets.


4. You can create new conditions and delete or modify the existing conditions.
To create a new condition:
 - a. Select an attribute.
 - b. Select an operator. For the ProducerIP, SrcIP, and DstIP attributes, you can choose the like, equals, or not-equals operator. For the other attributes, you can choose the =, !=, <=, or >= operator.
The Filter Text Configuration tab in the right pane shows the condition that you define in the Filter Details section. The All Filter Groups tab shows the list of all defined filter groups.
 - c. Specify the value to be compared.
 - d. Click **Add**. Another row of attributes and operators appears.
 - e. To add another condition, repeat the above steps. If you define multiple conditions, the NNM iSPI Performance for Traffic assigns the AND operator on them while performing the filtering action.
5. To modify an existing condition, modify the operator or the value to be compared from an existing condition.
6. To delete a condition, click **Remove** next to the condition.
7. If you like, you can change the group membership of the filter from the Group Membership of this Filter tab.

If you remove the group membership of the filter from every filter group, the NNM iSPI Performance for Traffic automatically places the filter in DefaultFilterGroup.
8. Click **Save & Close**.

Delete Filters

You can use the NNM iSPI Performance for Traffic Configuration form to delete existing filters.

To delete a filter:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Filters**.
2. In the Filters view, select the filter that you want to delete, and then click the  Delete icon. In the Filter Details section, select the filter operation.

Filter Groups

You can define filter groups to group a set of defined filters. The NNM iSPI Performance for Traffic provides you with a default filter group—DefaultFilterGroup.

You can use the Filter Mapping Groups view in the NNM iSPI Performance for Traffic Configuration form to define new filter groups, associate filters with existing filter groups, view and modify the existing filter groups, and delete filter groups.

To view the Filter Groups view, click **Filter Groups** in the NNM iSPI Performance for Traffic Configuration form.


The basic attributes of the Filter Groups view are the following:

Attributes	Description
Filter Group Name	The name of the group.
Number of Filters	The number of filters associated with the group.

Add a New Filter Group

The NNM iSPI Performance for Traffic provides you with a the default application mapping group—DefaultAppMapGroup. You can also define new application mapping groups by using the NNM iSPI Performance for Traffic Configuration form.


To add a new filter group:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Filter Groups**.
2. In the Filter Groups view, click the  Add icon. A new form opens.
3. In the Filter Group Details section, specify the name of the filter group. You can use alphanumeric characters, hyphens (-), and underscores (_).
4. The All Filters tab shows the list of all filters and their association with the filter groups. To associate a filter with the new filter group, select the select checkbox () next to the filter.
5. Click **Save & Close**.

Edit a Filter Group

You can edit a filter group's association with filters by using the NNM iSPI Performance for Traffic Configuration form. You cannot change the name of a filter group.

To edit a filter group:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Filter Groups**.
2. In the Filter Groups view, click the  Open icon. A new form opens. The Group Members of This Filter tab shows all the existing filters and their association with all the groups.
3. To associate a filter with the group, select the select checkbox () next to the filter. To dissociate a filter from the group, clear the select checkbox () next to the filter.


Before removing the group membership of a filter from the group, make sure the filter is already associated with at least one filter group. A filter cannot exist without a membership to a group, and therefore, is automatically deleted when you remove group membership from all existing groups by using this form.

4. Click **Save & Close**.

Delete a Filter Group

You can delete a filter group by using the NNM iSPI Performance for Traffic Configuration form.

To delete a filter group:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Filter Groups**.
2. In the Filter Groups view, select the filter group that you want to delete, and then click the  Delete icon.

Application Mapping

The application mapping feature enables you to associate flow packets with specific applications in your organization. This helps you correlate the flow packets with applications. The NNM iSPI Performance for Traffic provides you with a set of default application mapping definitions and a default application mapping group—DefaultAppMapGroup.

You can use the Application Mappings view in the NNM iSPI Performance for Traffic Configuration form to define new applications, map flow packets to existing applications, view and modify the current application mapping setting, and delete application definitions.

To view the Application Mappings view, click **Application Mappings** in the NNM iSPI Performance for Traffic Configuration form.


The basic attributes of the Application Mappings view are the following:

Attributes	Description
Application Name	The name of the application.
Condition Configuration	The expression that defines association of flow packets with an application.
Application Groups	Application mapping groups where the application belongs. An application can belong to multiple application groups.

Define a New Application

The NNM iSPI Performance for Traffic provides you with a set of default application mapping definitions and a default [application mapping group](#)—DefaultAppMapGroup. You can also define new applications by using the NNM iSPI Performance for Traffic Configuration form.

To define a new application:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Application Mappings**.
2. In the Application Mappings view, click the  Add icon. A new form opens with the following sections:
 - Application Mapping Details: In this section, you must specify the primary details of the application you want to add.
 - The other section lists related details.
3. In the Application Mapping Details section, specify the following details:
 - Application Name: Type the name of the application. You can use alphanumeric characters, hyphens (-), and underscores (_).
 - Define the mapping rule: The NNM iSPI Performance for Traffic enables you to map a flow packet to an application with the help of expressions created with different attributes of the

flow packet. The attributes are:

- ProducerIP: IP address of the system where the flow collector is located.
- SrcIP: IP address of the system where the traffic flow originated.
- DstIP: IP address of the system where the traffic flow terminated.
- IPProtocol: Protocol used by the traffic flow.
- NFSNMPInputIndex: SNMP index of the egress interface
- NFSNMPOutputIndex: SNMP index of the ingress interface
- DstPort: Ingress port
- TCPFlags: TCP flag of the traffic flow
- IPToS: Type of Service property of the traffic flow


To create an expression:

- a. Select an attribute.
 - b. Select an operator. For the ProducerIP, SrcIP, and DstIP attributes, you can choose the `like`, `equals`, or `not-equals` operator.
For other attributes, you can choose the `=`, `!=`, `<=`, or `>=` operator.
The Application Mapping Text Configuration tab in the right pane shows the condition that you define in the Filter Details section. The All Application Mapping Groups tab shows the list of all defined application mapping groups.
 - c. Specify the value to be compared.
 - d. Click **Add**. Another row of attributes and operators appears.
 - e. To add another expression, repeat the above steps. If you define multiple expressions, the NNM iSPI Performance for Traffic assigns the AND operator on them while performing the mapping action.
4. Click **Save & Close**.

Edit an Application Mapping Definition

You can use the NNM iSPI Performance for Traffic Configuration form to edit an existing application mapping definition.

To edit an application mapping definition:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Application Mappings**.
2. In the Application Mappings view, click the  Open icon. A new form opens with the following sections:
 - Application Mapping Details: In this section, you can modify the primary details of the application you want to add.
 - The other section lists related details.
3. In the Application Mapping Details section, you can modify the following details:
 - Application Name: You can modify the name of the application. You can use alphanumeric characters, hyphens (-), and underscores (_).

- Modify the mapping rule: The NNM iSPI Performance for Traffic enables you to map a flow packet to an application with the help of expressions created with different attributes of the flow packet. The attributes are:
 - ProducerIP: IP address of the system where the flow collector is located.
 - SrcIP: IP address of the system where the traffic flow originated.
 - DstIP: IP address of the system where the traffic flow terminated.
 - IPProtocol: Protocol used by the traffic flow.
 - NFSNMPInputIndex: SNMP index of the egress interface
 - NFSNMPOutputIndex: SNMP index of the ingress interface
 - DstPort: Ingress port
 - TCPFlags: TCP flag of the traffic flow
 - IPToS: Type of Service property of the traffic flow


To create an expression:

- a. Select an attribute.
 - b. Select an operator. For the ProducerIP, SrcIP, and DstIP attributes, you can choose the `like`, `equals`, or `not-equals` operator.
For other attributes, you can choose the `=`, `!=`, `<=`, or `>=` operator.
The Application Mapping Text Configuration tab in the right pane shows the condition that you define in the Filter Details section. The All Application Mapping Groups tab shows the list of all defined application mapping groups.
 - c. Specify the value to be compared.
 - d. Click **Add**. Another row of attributes and operators appears.
 - e. To add another expression, repeat the above steps. If you define multiple expressions, the NNM iSPI Performance for Traffic assigns the AND operator on them while performing the mapping action.
 - f. To remove an expression, click the **Remove** button next to the expression.
4. Click **Save & Close**.

Delete an Application

You can use the NNM iSPI Performance for Traffic Configuration form to delete an application mapping definition.

To delete an application:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Application Mappings**.
2. In the Application Mappings view, select the application that you want to delete.
3. Click the  Delete icon.

Application Mapping Groups

You can define application mapping groups to group a set of defined applications. Grouping applications into a group helps you analyze the data better as you can use the application groups as the Group By parameter on reports. The NNM iSPI Performance for Traffic provides you with a default application mapping group—DefaultAppMapGroup.

You can use the Application Mapping Groups view in the NNM iSPI Performance for Traffic Configuration form to define new application mapping groups, associate applications with existing application mapping groups, view and modify the current application mapping groups, and delete application mapping groups.

To view the Application Mapping Groups view, click **Application Mapping Groups** in the NNM iSPI Performance for Traffic Configuration form.


The basic attributes of the Application Mapping Groups view are the following:

Attributes	Description
Application Group	The name of the group.
Number of Application Mappings	The number of applications associated with the group.

Add a New Application Mapping Group

The NNM iSPI Performance for Traffic provides you with a the default application mapping group—DefaultAppMapGroup. You can also define new application mapping groups by using the NNM iSPI Performance for Traffic Configuration form.

To define a new application mapping group:


1. In the NNM iSPI Performance for Traffic Configuration form, click **Application Mapping Groups**.
2. In the Application Mapping Groups view, click the  Add icon. A new form opens.
3. In the Application Mapping Groups Details section, specify the name of the application mapping group. Follow these rules while naming an Application Mapping Group:
 - Use only alphabets to start an Application Mapping Group name.
 - Do **not** use numeric characters to start an Application Mapping Group name.
 - In the Application Mapping Group name, you can use alphanumeric characters, hyphens (-), and underscores (_). Do **not** use spaces or any other special characters

For example, you can create an Application Mapping Group called AppMap1Grp, but not 1AppMapGrp.
4. The All Application Mappings tab shows the list of all applications and their association with the application mapping groups. To associate an application with the new application mapping group, select the application.
5. Click **Save & Close**.

Edit an Application Mapping Group

You can edit an application mapping group's association with applications by using the NNM iSPI Performance for Traffic Configuration form. You cannot change the name of an application mapping group.

To edit an application mapping group:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Application Mapping Groups**.
2. In the Application Mapping Groups view, click  **Open**. A new form opens. The Application Mapping Group Members tab shows all the existing applications and their association with all the groups.
3. To associate an application with the group, select the application. To dissociate an application from the group, clear the select checkbox () next to the application.

Before removing the group membership of an application from the group, make sure the application is already associated with at least one application mapping group. An application cannot exist without a membership to a group, and therefore, is automatically deleted when you remove group membership from all existing groups by using this form.

You cannot remove an application from the application mapping group if the application belongs to the Top N inclusion list. If you try to remove the application from the application mapping group by clearing the checkbox () next to the application, the following message appears:

```
No changes done in application mapping group:<group_name> mapping group modified, but some of the application mappings that belong to the Inclusion List have not been removed.
```


To remove the application from the group, you must remove the application from the Top N Application Inclusion List first.

4. Click **Save & Close**.

Delete an Application Mapping Group

You can delete an application mapping group by using the NNM iSPI Performance for Traffic Configuration form.

To delete an application mapping group:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Application Mapping Groups**.
2. In the Application Mapping Groups view, select the application mapping group that you want to delete, and then click the  Delete icon.

Creating Filter Groups and Application Maps from the Command Line

With the help of the `nmstrafficfilterappmptool.ovpl` command, you can create filter groups and application mapping from the command line. The `nmstrafficfilterappmptool.ovpl` command accepts inputs from a text file (where the

definition for filter groups and application mapping exists) and creates filter groups and application mapping rules in the NNM iSPI Performance for Traffic configuration console.

To create filter groups:

1. Log on to the Master Collector system with the administrative or root privileges.
2. With the help of a text editor, create a new text file.
3. In the text file, add the following entry:
`<Condition_definition>, Action = <keep/drop> [, FilterGroups = <Filter_Group_Name>]`
In this instance:
`<Condition_definition>` is the condition defined on the flows.
`<Filter_Group_Name>` is the name of the filter group that you want to create.
Specify **keep** to retain the match.
Specify **drop** to discard the match.
You can specify multiple condition definitions separated by commas and multiple filter group names separated by spaces.
4. Save the file.
5. Go to the following directory:
`<TrafficMasterInstallDir>/bin`
6. Run the following command:
`nmstrafficfilterappmptool.ovpl --userName=<user name> --password=<password> --import <file name>`
In this instance:
`<user name>`: the user name to log on to the NNM iSPI Performance for Traffic configuration console
`<password>`: the password for the above user
`<file name>`: name of the text file that you created (specify the file name with the complete location).
The NNM iSPI Performance for Traffic creates the filter groups based on the definition provided in the text files and new groups appear in the configuration console.

To create application mapping:

1. Log on to the Master Collector system with the administrative or root privileges.
2. With the help of a text editor, create a new text file.
3. In the text file, add the following entry:
`<Condition definition>, App = <Application Name> [, AppGroups = <Application Group Name>]`
In this instance:
`<Condition_definition>` is the condition defined on the flows.
`<Application Name>` is the name of the application that you want to map to the expression.
Optional. `<Application Group Name>` is the group name for the application.
You can specify multiple condition definitions separated by commas and multiple application names separated by spaces.
4. Save the file.
5. Go to the following directory:
`<TrafficMasterInstallDir>/bin`

6. Run the following command:
nmstrafficfilterappmptool.ovpl --userName=<user name> --password=<password> --import <file name>
In this instance:
<user name>: the user name to log on to the NNM iSPI Performance for Traffic configuration console
<password>: the password for the above user
<file name>: name of the text file that you created (specify the file name with the complete location).
The NNM iSPI Performance for Traffic creates the filter groups based on the definition provided in the text files and new groups appear in the configuration console.


Configure Classes of Service

The NNM iSPI Performance for Traffic enables you to enrich every traffic flow by adding the Class of Service attribute to the flow. You can define this attribute by using the NNM iSPI Performance for Traffic Configuration form. If defined, you can sort or group different values of traffic metrics on reports by this attribute.

Add Class of Service Definitions

To use the Class of Service property to rank traffic metric values, you must define Classes of Service first by using the NNM iSPI Performance for Traffic Configuration form.


To define a class of service:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Type Of Service Groups**.
2. In the Type Of Service Groups view, click the  Add icon. A new form opens.
3. In the new form, follow these steps:
 - a. In the TOS Group Name box, type a name. While configuring a Leaf Collector instance (see ["Add a Leaf Collector Instance" \(on page 16\)](#)), you can associate this TOS group name with the Leaf Collector.
 - b. In the Type Of Service Group Details section, select a Type of Service (ToS) value, select an operation (= or *between*), and then select a ToS value (select two values if you choose the *between* operation).
 - c. In the Operand box, type the name of the class of service. This class of service name appears in the 'Grouping By' metric list on reports if you associate the TOS group with a Leaf Collector instance.
 - d. If you want to add another class of service, click **Add**, and then repeat [step c](#).
4. Click **Save & Close**. The newly defined TOS group appears in the Type Of Service Groups view.

Edit Class of Service Definitions

You can modify the existing Class of Service definitions by using the NNM iSPI Performance for Traffic Configuration form.


To edit a class of service:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Type Of Service Groups**.
2. In the Type Of Service Groups view, select a TOS group, and then click the  Open icon. A new form opens.
3. In the new form, follow these steps:
 - a. In the Type Of Service Group Details section, modify existing class of service definitions by changing the Type of Service (ToS) value or operation (= or *between*).
 - b. In the Operand box, you can change the name of the class of service.
 - c. If you want to add another class of service, click **Add**. If you want to remove an existing class of service, click **Remove**.
4. Click **Save & Close**.

Delete TOS Groups

By using the NNM iSPI Performance for Traffic Configuration form, you can delete TOS groups that you have created.

To delete a TOS group:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Type Of Service Groups**.
2. In the Type Of Service Groups view, select the TOS group that you want to delete, and then click the  Delete icon.

Top N Application Inclusion List

The Top N Application Inclusion List view enables you to configure the NNM iSPI Performance for Traffic to always include select applications on the Top N reports in Interface_1_min and Interface_15_min report folders. Typically in leaf collector only top contributors to traffic are retained for a time interval and the rest are grouped into a single 'Anonymous' bucket. In the case of applications, you can configure a set of applications such that traffic data for them will always be retained irrespective of their contribution to the traffic volume.

To open the Top N Application Inclusion List view, open the NNM iSPI Performance for Traffic Configuration form, and then click **Top N Application Inclusion List**.

To add an application to the list of applications that always appear on Top N reports:

1. Select an application mapping group.
2. From the left pane, select the applications that you want to add to the list.
3. Click **Add**. The selected applications appear on every Top N report.

To remove an application from the list, select the application from the right pane, and then click **Remove**.

If you define multiple applications with the same name, the NNM iSPI Performance for Traffic Configuration form lets you add only one application from among the applications with the same name.

Configuring Threshold to Monitor Traffic Flow

NNM iSPI Performance for Traffic thresholds enable you to monitor the volume of traffic passing through an interface. Use Threshold Configuration feature to specify the set of interfaces for which you want to monitor threshold. You can select a group of interfaces, all interfaces in a selected node, or all interfaces for a selected site for threshold configuration. NNM iSPI Performance for Traffic monitors each interface of the node or site individually based on the configured threshold.

NNM iSPI Performance for Traffic uses the following metrics for threshold monitoring.

- **Volume:** Refers to the number of bytes flowing through the interface. The units that NNM iSPI Performance for Traffic uses to measure the traffic volume are Bytes, Kilobytes, Megabytes, and Gigabytes.
- **Application Bandwidth:** Refers to the bandwidth consumed by an application on an interface. The units that NNM iSPI Performance for Traffic uses to measure the traffic bandwidth are bps, Kbps, Mbps, and Gbps.

Note: The above metrics are applied to both ingress and egress traffic flows and both are monitored for threshold violations.

NNM iSPI Performance for Traffic computes the metric values for the selected set of thresholds every five minutes. It generates or clears the incidents based on the computed values and configured threshold values.

NNM iSPI Performance for Traffic performs the following actions if the threshold for an interface is breached:

- Creates an incident for the breached threshold
For information on incident types supported by NNM iSPI Performance for Traffic, see [Incident Types Supported](#).
- Updates the threshold state of the interface in Flow Interfaces view
- Updates the threshold state of the related node

For example, if you have configured a threshold on the Interface Fa0/0 of Node A, and the traffic volume passing through Interface Fa0/0 crosses the threshold value, NNM iSPI Performance for Traffic automatically raises an incident and updates the threshold state for the following:

- Flow interface Fa0/0
- Hosting node Node A

When the traffic volume comes back to the acceptable range, NNM iSPI Performance for Traffic clears the incident and updates the status of the flow interface and the node accordingly.

The following workspaces enable you to view the interfaces and nodes affected by a threshold:

- [Threshold Exceptions Reporting Interfaces](#)
- [Threshold Exceptions Reporting Nodes](#)





Launching the Threshold Configuration Panel

To launch the threshold configuration form:

1. Log on to HP Network Node Manager i Software (NNMi) console using your username and password.
You must have administrator privileges.
2. Click **Configuration**. The Configuration tab expands.
3. Select **NNM iSPI Performance for Traffic Configuration**
4. On the Configuration panel, click **Threshold**.


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

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

Available Threshold Configuration Tools	Description
	Enable you to create a new threshold
	Performs the following operations: <ul style="list-style-type: none"> • Opens the Threshold Details form for the selected threshold. • Enables you to edit the selected threshold configuration.
	Deletes the selected threshold
	Retrieves the last saved threshold configuration from the database and displays the configured thresholds in the Threshold Configuration panel.

Adding New Threshold Settings Using the Threshold Details Form

To add a new threshold:

1. [Launch the Threshold Configuration panel](#).
2. Click  **New** in Threshold Configuration panel to open the Threshold Details form.
3. NNM iSPI Performance for Traffic assigns the new threshold to the interfaces configured for an existing group of interfaces , nodes, or sites. Specify the following information in the Threshold Details form:

Field Name	Description
Metric	<p>Select any of the following metric for the threshold:</p> <ul style="list-style-type: none"> Volume:¹ Bandwidth:³
High Value	<p>Type a high value for the threshold.</p> <ul style="list-style-type: none"> If you have selected Volume in the metric field, you can select Bytes, MB, or GB for the threshold. If you have selected Bandwidth in the metric field, you can select bps, Kbps, Mbps, or Gbps for the threshold. <p>If the traffic volume or data bandwidth for the interfaces cross this high value, NNM iSPI Performance for Traffic creates an NNMi incident and updates the status for the node for which the interfaces are configured.</p>
High Rearm Value	<p>Type a high rearm value for the threshold.</p> <p>The high rearm value specifies the acceptable range of traffic volume or data bandwidth for the selected interfaces.</p> <p>NNM iSPI Performance for Traffic performs the following tasks once the traffic volume or data bandwidth for the selected interfaces reach the high rearm value:</p> <ul style="list-style-type: none"> Updates the life-cycle state of the NNMi incident to Closed state Updates the node status
Application or ToS - Set Threshold By	<p>Select any of the following types for the threshold:</p> <ul style="list-style-type: none"> Application: Select this option if you want NNM iSPI Performance for Traffic to monitor each application for each of the selected interfaces. <p>If you select Bandwidth as the threshold metric, you can select either Application or All Applications as the threshold type.</p> <p>On the Application Mappings tab, select the application names that you want to monitor. Make sure that you select at least one application.</p> <ul style="list-style-type: none"> All Applications: Select this option if you want NNM iSPI Performance for Traffic to monitor all applications for each of the selected interfaces.

¹ Selecting this metric enables the threshold to monitor the volume of traffic passing through the [selected interfaces](#)²

² Selected interfaces for a threshold could specify the interfaces in the selected interface group, or the interfaces configured for the selected node or site.

³ Selecting this metric enables the threshold to monitor the application bandwidth for the selected interfaces.

	<p>If you select Bandwidth as the threshold metric, you can select either Application or All Applications as the threshold type.</p> <ul style="list-style-type: none"> ■ ToS: Select this option if you want NNM iSPI Performance for Traffic to monitor each class of service for each of the selected interfaces. Make sure that you select this threshold type if you have selected Volume as the threshold metric. <p>On the Type of Service Mappings tab, select the class of service names that you want to monitor. Make sure that you select at least one class of service.</p> <ul style="list-style-type: none"> ■ All ToS: Select this option if you want NNM iSPI Performance for Traffic to monitor all classes of service for each of the selected interfaces. Make sure that you select this threshold type if you have selected Volume as the threshold metric. ■ None: Select this option if you want NNM iSPI Performance for Traffic to monitor the total volume of traffic passing through each interface in the selected interface group, node, or site. NNM iSPI Performance for Traffic monitors the traffic volume across all applications and classes of services if you select this option. You can select this option only if you have selected Volume as the threshold metric. <p>On the Type of Service Mappings tab, if the ToS Operator column displays the value EQUALS, the ToS Second Number column displays the value -1.</p> <p>The ToS Second Number column displays the upper ToS range only if the ToS Operator column displays the value IN. The value IN specifies that you have selected 'between' in the Operation field while creating the ToS group. For more information about creating ToS groups, see Add Class of Service Definitions.</p>
<p>Topology Filters - Set Threshold By</p>	<p>Select one of the following options to select a topology filter for the threshold:</p> <ul style="list-style-type: none"> ■ Interface: Select this option if you want the threshold to monitor a group of interfaces. <p>On the Flow Enabled Interfaces tab, select the interfaces for the threshold.</p> <ul style="list-style-type: none"> ■ Node: Select this option if you want the threshold to monitor all the interfaces configured for a selected node. <p>On the Flow Enabled Nodes tab, select the nodes for the threshold. The threshold monitors all interfaces configured for the selected nodes.</p> <ul style="list-style-type: none"> ■ Site: Select this option if you want the threshold to monitor all the interfaces configured for a selected site. <p>On the Sites tab, select the sites for the threshold. The threshold monitors all interfaces configured for the all nodes in the selected sites.</p>

4. Click **Save and Close** to save the threshold configuration and close the Threshold Details form.

If you do not select any value in the Application or ToS and Topology Filters section, the configured threshold applies to all applications, ToS, interfaces, nodes, and sites that NNM iSPI Performance for Traffic uses.

Adding New Threshold Settings for Interfaces Using the Traffic Analysis Workspace

You can use the views displayed in the Traffic Analysis workspace to configure thresholds for interfaces.

To add a new threshold for an interface:

1. In the **Workspaces** navigation pane, select the **Traffic Analysis** workspace.
2. Select any of the following views:
 - Traffic Reporting Interfaces
 - Threshold Exceptions Reporting Interfaces
3. Right click on a interface and select **Configure Traffic Threshold** to open the Threshold Details form.
4. NNM iSPI Performance for Traffic assigns the new threshold to the interface that you selected in the view. Specify the following information in the Threshold Details form:

Field Name	Description
Metric	Select any of the following metric for the threshold: <ul style="list-style-type: none"> ■ Volume:¹ ■ Bandwidth:³
High Value	Type a high value for the threshold. <ul style="list-style-type: none"> ■ If you have selected Volume in the metric field, you can select Bytes, MB, or GB for the threshold. ■ If you have selected Bandwidth in the metric field, you can select bps, Kbps, Mbps, or Gbps for the threshold. <p>If the traffic volume or data bandwidth for the interfaces cross this high value, NNM iSPI Performance for Traffic creates an NNMi incident and updates the status for the node for which the interfaces are configured.</p>
High Rearm Value	Type a high rearm value for the threshold. The high rearm value specifies the acceptable range of traffic volume or data bandwidth for the selected interfaces.

¹ Selecting this metric enables the threshold to monitor the volume of traffic passing through the [selected interfaces](#)²

² Selected interfaces for a threshold could specify the interfaces in the selected interface group, or the interfaces configured for the selected node or site.

³ Selecting this metric enables the threshold to monitor the application bandwidth for the selected interfaces.

	<p>NNM iSPI Performance for Traffic performs the following tasks once the traffic volume or data bandwidth for the selected interfaces reach the high rearm value:</p> <ul style="list-style-type: none"> ■ Updates the life-cycle state of the NNMi incident to Closed state ■ Updates the node status
<p>Application or ToS - Set Threshold By</p>	<p>Select any of the following types for the threshold:</p> <ul style="list-style-type: none"> ■ Application: Select this option if you want NNM iSPI Performance for Traffic to monitor each application for each of the selected interfaces. If you select Bandwidth as the threshold metric, you can select either Application or All Applications as the threshold type. On the Application Mappings tab, select the application names that you want to monitor. Make sure that you select at least one application. ■ All Applications: Select this option if you want NNM iSPI Performance for Traffic to monitor all applications for each of the selected interfaces. If you select Bandwidth as the threshold metric, you can select either Application or All Applications as the threshold type. ■ ToS: Select this option if you want NNM iSPI Performance for Traffic to monitor each class of service for each of the selected interfaces. Make sure that you select this threshold type if you have selected Volume as the threshold metric. On the Type of Service Mappings tab, select the class of service names that you want to monitor. Make sure that you select at least one class of service. ■ All ToS: Select this option if you want NNM iSPI Performance for Traffic to monitor all classes of service for each of the selected interfaces. Make sure that you select this threshold type if you have selected Volume as the threshold metric. ■ None: Select this option if you want NNM iSPI Performance for Traffic to monitor the total volume of traffic passing through each interface in the selected interface group, node, or site. NNM iSPI Performance for Traffic monitors the traffic volume across all applications and classes of services if you select this option. You can select this option only if you have selected Volume as the threshold metric. <p>On the Type of Service Mappings tab, if the ToS Operator column displays the value EQUALS, the ToS Second Number column displays the value -1.</p> <p>The ToS Second Number column displays the upper ToS range only if the ToS Operator column displays the value IN. The value IN specifies that you have selected 'between' in the Operation field while creating the ToS group. For more information about creating ToS groups, see Add Class of Service Definitions.</p>

Topology Filters - Set Threshold By	<p>NNM iSPI Performance for Traffic automatically selects the option Interface when you create the threshold from the Traffic Analysis interface views.</p> <p>The interface that you selected in the Traffic Analysis interface view appears as selected in the Flow Enabled Interfaces tab.</p>
-------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

5. Select any of the following options:

- Save and Close:¹
- Save and New:²

To add a new threshold for a site:

1. In the **Workspaces** navigation pane, select the **Traffic Analysis** workspace.
2. Select the **Traffic Sites** view.
3. Right click on a site and select **Configure Traffic Threshold** to open the Threshold Details form.
4. NNM iSPI Performance for Traffic assigns the new threshold to the interfaces configured for the site that you selected in the view. Specify the following information in the Threshold Details form:

Field Name	Description
Threshold Name	Enter a unique name for the threshold. NNM iSPI Performance for Traffic identifies the threshold by its name.
Metric	<p>Select any of the following metric for the threshold:</p> <ul style="list-style-type: none"> ■ Volume:³ ■ Bandwidth:⁵
High Value	Type a high value for the threshold.

¹ Click this button to save the threshold configuration and close the Threshold Details form.

² Click this button to save the threshold configuration and refresh the Threshold Details form and create a new threshold.

³ Selecting this metric enables the threshold to monitor the volume of traffic passing through the [selected interfaces](#)⁴

⁴ Selected interfaces for a threshold could specify the interfaces in the selected interface group, or the interfaces configured for the selected node or site.

⁵ Selecting this metric enables the threshold to monitor the application bandwidth for the selected interfaces.

	<ul style="list-style-type: none"> ■ If you have selected Volume in the metric field, you can select Bytes, MB, or GB for the threshold. ■ If you have selected Bandwidth in the metric field, you can select bps, Kbps, Mbps, or Gbps for the threshold. <p>If the traffic volume or data bandwidth for the interfaces cross this high value, NNM iSPI Performance for Traffic creates an NNMi incident and updates the status for the node for which the interfaces are configured.</p>
<p>High Rearm Value</p>	<p>Type a high rearm value for the threshold.</p> <p>The high rearm value specifies the acceptable range of traffic volume or data bandwidth for the selected interfaces.</p> <p>NNM iSPI Performance for Traffic performs the following tasks once the traffic volume or data bandwidth for the selected interfaces reach the high rearm value:</p> <ul style="list-style-type: none"> ■ Updates the life-cycle state of the NNMi incident to Closed state ■ Updates the node status
<p>Application or ToS - Set Threshold By</p>	<p>Select any of the following types for the threshold:</p> <ul style="list-style-type: none"> ■ Application: Select this option if you want NNM iSPI Performance for Traffic to monitor each application for each of the selected interfaces. <p>If you select Bandwidth as the threshold metric, you can select either Application or All Applications as the threshold type.</p> <p>On the Application Mappings tab, select the application names that you want to monitor. Make sure that you select at least one application.</p> <ul style="list-style-type: none"> ■ All Applications: Select this option if you want NNM iSPI Performance for Traffic to monitor all applications for each of the selected interfaces. <p>If you select Bandwidth as the threshold metric, you can select either Application or All Applications as the threshold type.</p> <ul style="list-style-type: none"> ■ ToS: Select this option if you want NNM iSPI Performance for Traffic to monitor each class of service for each of the selected interfaces. Make sure that you select this threshold type if you have selected Volume as the threshold metric. <p>On the Type of Service Mappings tab, select the class of service names that you want to monitor. Make sure that you select at least one class of service.</p> <ul style="list-style-type: none"> ■ All ToS: Select this option if you want NNM iSPI Performance for Traffic to monitor all classes of service for each of the selected interfaces. Make sure that you select this threshold type if you have selected Volume as the threshold metric.

	<ul style="list-style-type: none"> ■ None: Select this option if you want NNM iSPI Performance for Traffic to monitor the total volume of traffic passing through each interface in the selected interface group, node, or site. NNM iSPI Performance for Traffic monitors the traffic volume across all applications and classes of services if you select this option. You can select this option only if you have selected Volume as the threshold metric. <p>On the Type of Service Mappings tab, if the ToS Operator column displays the value EQUALS, the ToS Second Number column displays the value -1.</p> <p>The ToS Second Number column displays the upper ToS range only if the ToS Operator column displays the value IN. The value IN specifies that you have selected 'between' in the Operation field while creating the ToS group. For more information about creating ToS groups, see Add Class of Service Definitions.</p>
<p>Topology Filters - Set Threshold By</p>	<p>NNM iSPI Performance for Traffic automatically selects the option Site when you create the threshold from the Traffic Sites view in the Traffic Analysis workspace.</p> <p>The site that you selected in the Traffic Sites view appears as selected in the Sites tab.</p>

5. Click **Save and Close** to save the threshold configuration and close the Threshold Details form.

If you do not select any value in the Application or ToS and Topology Filters section, the configured threshold applies to all applications, ToS, interfaces, nodes, and sites that NNM iSPI Performance for Traffic uses.

Adding New Threshold Settings for Nodes Using the Traffic Analysis Workspace

You can use the views displayed in the Traffic Analysis workspace to configure thresholds for nodes.

To add a new threshold for a node:

1. In the **Workspaces** navigation pane, select the **Traffic Analysis** workspace.
2. Select any of the following views:
 - Traffic Reporting Nodes
 - Threshold Exceptions Reporting Nodes
3. Right click on a node and select **Configure Traffic Threshold** to open the Threshold Details form.
4. NNM iSPI Performance for Traffic assigns the new threshold to the interfaces configured for the node that you selected in the view. Specify the following information in the Threshold Details form:

Field Name	Description
Metric	<p>Select any of the following metric for the threshold:</p> <ul style="list-style-type: none"> ■ Volume:¹ ■ Bandwidth:³
High Value	<p>Type a high value for the threshold.</p> <ul style="list-style-type: none"> ■ If you have selected Volume in the metric field, you can select Bytes, MB, or GB for the threshold. ■ If you have selected Bandwidth in the metric field, you can select bps, Kbps, Mbps, or Gbps for the threshold. <p>If the traffic volume or data bandwidth for the interfaces cross this high value, NNM iSPI Performance for Traffic creates an NNMi incident and updates the status for the node for which the interfaces are configured.</p>
High Rearm Value	<p>Type a high rearm value for the threshold.</p> <p>The high rearm value specifies the acceptable range of traffic volume or data bandwidth for the selected interfaces.</p> <p>NNM iSPI Performance for Traffic performs the following tasks once the traffic volume or data bandwidth for the selected interfaces reach the high rearm value:</p> <ul style="list-style-type: none"> ■ Updates the life-cycle state of the NNMi incident to Closed state ■ Updates the node status
Application or ToS - Set Threshold By	<p>Select any of the following types for the threshold:</p> <ul style="list-style-type: none"> ■ Application: Select this option if you want NNM iSPI Performance for Traffic to monitor each application for each of the selected interfaces. <p>If you select Bandwidth as the threshold metric, you can select either Application or All Applications as the threshold type.</p> <p>On the Application Mappings tab, select the application names that you want to monitor. Make sure that you select at least one application.</p>

¹ Selecting this metric enables the threshold to monitor the volume of traffic passing through the [selected interfaces](#)²

²Selected interfaces for a threshold could specify the interfaces in the selected interface group, or the interfaces configured for the selected node or site.

³Selecting this metric enables the threshold to monitor the application bandwidth for the selected interfaces.

	<ul style="list-style-type: none"> ■ All Applications: Select this option if you want NNM iSPI Performance for Traffic to monitor all applications for each of the selected interfaces. If you select Bandwidth as the threshold metric, you can select either Application or All Applications as the threshold type. ■ ToS: Select this option if you want NNM iSPI Performance for Traffic to monitor each class of service for each of the selected interfaces. Make sure that you select this threshold type if you have selected Volume as the threshold metric. On the Type of Service Mappings tab, select the class of service names that you want to monitor. Make sure that you select at least one class of service. ■ All ToS: Select this option if you want NNM iSPI Performance for Traffic to monitor all classes of service for each of the selected interfaces. Make sure that you select this threshold type if you have selected Volume as the threshold metric. ■ None: Select this option if you want NNM iSPI Performance for Traffic to monitor the total volume of traffic passing through each interface in the selected interface group, node, or site. NNM iSPI Performance for Traffic monitors the traffic volume across all applications and classes of services if you select this option. You can select this option only if you have selected Volume as the threshold metric. <p>On the Type of Service Mappings tab, if the ToS Operator column displays the value EQUALS, the ToS Second Number column displays the value -1.</p> <p>The ToS Second Number column displays the upper ToS range only if the ToS Operator column displays the value IN. The value IN specifies that you have selected 'between' in the Operation field while creating the ToS group. For more information about creating ToS groups, see Add Class of Service Definitions.</p>
<p>Topology Filters - Set Threshold By</p>	<p>NNM iSPI Performance for Traffic automatically selects the option Node when you create the threshold from the Traffic Analysis node views.</p> <p>The node that you selected in the Traffic Analysis node view appears as selected in the Flow Enabled Nodes tab.</p>

5. Click **Save and Close** to save the threshold configuration and close the Threshold Details form.

If you do not select any value in the Application or ToS and Topology Filters section, the configured threshold applies to all applications, ToS, interfaces, nodes, and sites that NNM iSPI Performance for Traffic uses.

Adding New Threshold Settings for Sites Using the Traffic Analysis Workspace

You can use the views displayed in the Traffic Analysis workspace to configure thresholds for sites.

To add a new threshold for a site:

1. In the **Workspaces** navigation pane, select the **Traffic Analysis** workspace.
2. Select the **Traffic Sites** view.
3. Right click on a site and select **Configure Traffic Threshold** to open the Threshold Details form.
4. NNM iSPI Performance for Traffic assigns the new threshold to the interfaces configured for the site that you selected in the view. Specify the following information in the Threshold Details form:

Field Name	Description
Metric	<p>Select any of the following metric for the threshold:</p> <ul style="list-style-type: none"> ■ Volume:¹ ■ Bandwidth:³
High Value	<p>Type a high value for the threshold.</p> <ul style="list-style-type: none"> ■ If you have selected Volume in the metric field, you can select Bytes, MB, or GB for the threshold. ■ If you have selected Bandwidth in the metric field, you can select bps, Kbps, Mbps, or Gbps for the threshold. <p>If the traffic volume or data bandwidth for the interfaces cross this high value, NNM iSPI Performance for Traffic creates an NNMi incident and updates the status for the node for which the interfaces are configured.</p>
High Rearm Value	<p>Type a high rearm value for the threshold.</p> <p>The high rearm value specifies the acceptable range of traffic volume or data bandwidth for the selected interfaces.</p> <p>NNM iSPI Performance for Traffic performs the following tasks once the traffic volume or data bandwidth for the selected interfaces reach the high rearm value:</p> <ul style="list-style-type: none"> ■ Updates the life-cycle state of the NNMi incident to Closed state ■ Updates the node status
Application or ToS - Set	<p>Select any of the following types for the threshold:</p>

¹ Selecting this metric enables the threshold to monitor the volume of traffic passing through the [selected interfaces](#)²

²Selected interfaces for a threshold could specify the interfaces in the selected interface group, or the interfaces configured for the selected node or site.

³Selecting this metric enables the threshold to monitor the application bandwidth for the selected interfaces.

<p>Threshold By</p>	<ul style="list-style-type: none"> ■ Application: Select this option if you want NNM iSPI Performance for Traffic to monitor each application for each of the selected interfaces. If you select Bandwidth as the threshold metric, you can select either Application or All Applications as the threshold type. On the Application Mappings tab, select the application names that you want to monitor. Make sure that you select at least one application. ■ All Applications: Select this option if you want NNM iSPI Performance for Traffic to monitor all applications for each of the selected interfaces. If you select Bandwidth as the threshold metric, you can select either Application or All Applications as the threshold type. ■ ToS: Select this option if you want NNM iSPI Performance for Traffic to monitor each class of service for each of the selected interfaces. Make sure that you select this threshold type if you have selected Volume as the threshold metric. On the Type of Service Mappings tab, select the class of service names that you want to monitor. Make sure that you select at least one class of service. ■ All ToS: Select this option if you want NNM iSPI Performance for Traffic to monitor all classes of service for each of the selected interfaces. Make sure that you select this threshold type if you have selected Volume as the threshold metric. ■ None: Select this option if you want NNM iSPI Performance for Traffic to monitor the total volume of traffic passing through each interface in the selected interface group, node, or site. NNM iSPI Performance for Traffic monitors the traffic volume across all applications and classes of services if you select this option. You can select this option only if you have selected Volume as the threshold metric. <p>On the Type of Service Mappings tab, if the ToS Operator column displays the value EQUALS, the ToS Second Number column displays the value -1.</p> <p>The ToS Second Number column displays the upper ToS range only if the ToS Operator column displays the value IN. The value IN specifies that you have selected 'between' in the Operation field while creating the ToS group. For more information about creating ToS groups, see Add Class of Service Definitions.</p>
<p>Topology Filters - Set Threshold By</p>	<p>NNM iSPI Performance for Traffic automatically selects the option Site when you create the threshold from the Traffic Sites view in the Traffic Analysis workspace.</p> <p>The site that you selected in the Traffic Sites view appears as selected in the Sites tab.</p>

5. Click **Save and Close** to save the threshold configuration and close the Threshold Details form.


If you do not select any value in the Application or ToS and Topology Filters section, the configured threshold applies to all applications, ToS, interfaces, nodes, and sites that NNM iSPI Performance for Traffic uses.

Modifying Threshold Settings Using the Threshold Details Form

To modify an existing threshold:

1. [Launch the Threshold Configuration panel.](#)
2. Select the threshold that you want to modify.

You can select multiple thresholds. NNM iSPI Performance for Traffic displays each threshold in a separate Threshold Details form.

3. Click  in Threshold Configuration panel to open the Threshold Details form.
4. You can modify only the following values for an existing threshold:

Field Name	Description
High Value	<p>Type a high value for the threshold.</p> <ul style="list-style-type: none"> ■ If you have selected Volume in the metric field, you can select Bytes, MB, or GB for the threshold. ■ If you have selected Bandwidth in the metric field, you can select bps, Kbps, Mbps, or Gbps for the threshold. <p>If the traffic volume or data bandwidth for the interfaces cross this high value, NNM iSPI Performance for Traffic creates an NNMi incident and updates the status for the node for which the interfaces are configured.</p>
High Rearm Value	<p>Type a high rearm value for the threshold.</p> <p>The high rearm value specifies the acceptable range of traffic volume or data bandwidth for the selected interfaces.</p> <p>NNM iSPI Performance for Traffic performs the following tasks once the traffic volume or data bandwidth for the selected interfaces reach the high rearm value:</p> <ul style="list-style-type: none"> ■ Updates the life-cycle state of the NNMi incident to Closed state ■ Updates the node status


5. Click the **Save and Close** button to save the modified threshold configuration and close the Threshold Details form.

While creating the threshold, if you did not select any value in the Topology Filters section, NNM iSPI Performance for Traffic applies the threshold to all applications, ToS, interfaces, nodes, and sites. In such scenario, the Threshold Details form does not display any value in the following tabs:

- Sites
- Flow Node/Interface
- Type of service Mappings
- Application Mappings

Deleting Threshold Settings Using the Threshold Details Form

To delete an existing threshold:

1. [Launch the Threshold Configuration panel.](#)
2. Select the threshold that you want to delete.
You can select multiple thresholds for deletion.
3. Click  in Threshold Configuration panel.
4. Click **Delete** to delete the selected thresholds.

NNM iSPI Performance for Traffic performs the following tasks when you delete a threshold:



- Rearms all the related incidents in the Exceeded state. Rearming the incidents sets the incident state to Normal state.
- Sets the node state to Normal state if all the incidents belonging to the node are set to the Normal state.

Chapter 3

Diagnosing the Health of the NNM iSPI Performance for Traffic

The Traffic Health view helps you monitor the health of the NNM iSPI Performance for Traffic. The view presents a comprehensive list of all the problems encountered by the selected NNM iSPI Performance for Traffic leaf collector during its operation.

To open the Traffic Health view:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Traffic Health**.
2. Click  **Refresh** to refresh the list of leaf collectors available on the view.
3. Select a leaf collector and click  to open the Traffic Health view for the leaf collector.

The basic attributes of the view are the following:

Attributes	Description
Problem ID	ID of the problem encountered by the NNM iSPI Performance for Traffic
Severity	Severity of the problem
Start Time	Time when the problem started
End Time	Time when the problem got resolved
Status	Status of the problem
Message	Problem description
Suggestion	Suggestions to resolve the problem

Verifying the Installation Configuration Parameters for Master Collector

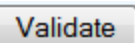
For error-free performance, make sure that NNM iSPI Performance for Traffic can communicate with the following applications and application components:

- NNMi
- NPS
- Shared drive between NNMi, NPS, and NNM iSPI Performance for Traffic Master Collector.
- Secondary NNMi Server (if you have configured NNM iSPI Performance for Traffic for high availability)

If the secondary NNMi server is configured correctly, NNM iSPI Performance for Traffic may work even if the primary NNMi server is not configured correctly.

NNM iSPI Performance for Traffic Installation Verification form enables you to view, verify and modify the configuration parameters that you entered while installing NNM iSPI Performance for Traffic Master Collector.

The form displays the status of each configuration category.

Click  **Validate** to display the invalid configuration settings in red and the highlight the invalid configuration settings.

To modify a configuration parameter:


1. On the Installation Verification form, click  **Edit** to modify the value for any of the following parameters:

NNM iSPI Performance for Traffic Installation Verification form lists the following parameters:

Parameter Title	Parameter Detail	Details Description
Primary NNMi Server Details		
NNM HTTPS Port	com.hp.ov.nms.spi.traffic-master.Nnm.https.port	The HTTPS port that the primary NNMi server uses to communicate with NNM iSPI Performance for Traffic Master Collector
NNM Password	com.hp.ov.nms.spi.traffic-master.Nnm.password	The administrator password for the primary NNMi server
NNM Username	com.hp.ov.nms.spi.traffic-master.Nnm.username	The administrator username for the primary NNMi server
NNM Hostname	com.hp.ov.nms.spi.traffic-master.Nnm.hostname	The Fully Qualified Domain Name (FQDN) for the primary NNMi server
NNM HTTP Port	com.hp.ov.nms.spi.traffic-master.Nnm.port	The HTTP Port that the primary NNMi server uses to communicate with NNM iSPI Performance for Traffic Master Collector
Secondary NNMi Server Details (Applicable Only If NNM iSPI Performance for Traffic is Configured for High Availability)		
NNM SECONDARY Username	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.username	The administrator username for the secondary NNMi server
NNM SECONDARY HTTPS Port	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.https.port	The HTTPS port that the secondary NNMi server uses to communicate with NNM iSPI Performance for Traffic

		Master Collector
NNM SECONDARY Hostname	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.hostname	The Fully Qualified Domain Name (FQDN) for the secondary NNMi server
NNM SECONDARY Present	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.present	Specifies whether the secondary NNMi server is configured for High Availability and Application Failover True if Secondary NNM has been configured and failover enabled
NNM SECONDARY HTTP Port	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.port	The HTTP port that the secondary NNMi server uses to communicate with NNM iSPI Performance for Traffic Master Collector
NNM SECONDARY Password	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.password	The administrator password for the secondary NNMi server
Primary Shared Drive Details		
NNM SPI Data Path	com.hp.ov.nms.spi.traffic-master.Nnm.perfspidatapath	The shared folder on the primary NNMi server that the Master Collector and NPS use for storing the data collected by NNM iSPI Performance for Traffic
Secondary Shared Drive Details (Applicable Only If NNM iSPI Performance for Traffic is Configured for High Availability)		
NNM SECONDARY SPI Data Path	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.perfspidatapath	The shared folder on the secondary NNMi server that the Master Collector and NPS use for storing the data collected by NNM iSPI Performance for Traffic
NPS Details		
NPS Port	com.hp.ov.nms.spi.traffic-master.nps.port	The port that the Master Collector uses to communicate with the NPS server NPS and NNM iSPI Performance for Traffic must use same mode of communication protocol. That is, if NPS uses HTTPS, NNM iSPI Performance for Traffic must also use HTTPS protocol.
NPS Sybase Username	com.hp.ov.nms.spi.traffic-master.nps.sybase.user	The administrator username for the NPS database

NPS Sybase Password	com.hp.ov.nms.spi.traffic-master.nps.sybase.password	The administrator password for the NPS database
NPS Hostname	com.hp.ov.nms.spi.traffic-master.nps.hostname	The Fully Qualified Domain Name (FQDN) for the system where NPS and NNM iSPI Performance for Metrics are installed

2. Specify the configuration value in the Value field.
3. Click  **Save** to save the modified value.
4. NNM iSPI Performance for Traffic validates your changes. If the values you specified are incorrect, the Installation Verification form displays an error message for the incorrect configuration setting.
5. Restart the NNM iSPI Performance for Traffic Master Collector to apply the changes.

Note: Using this form, you can update the configuration parameters defined in the following properties files:

- nnm.extended.properties
- nps.extended.properties
- nms-traffic-master.address.properties

You can find these properties files in the following location:

Windows: <Ov_Data_Dir>\shared\nmsas\traffic-master\conf\

Linux: \$OvDataDir/shared/nmsas/traffic-master/conf/


Viewing Unresolved IPs

You can view IP addresses of interfaces (which are capable of reporting the traffic flow data) that the NNM iSPI Performance for Traffic failed to resolve. The Unresolved NNM IP view in the NNM iSPI Performance for Traffic Configuration form enables you to view the list of IP addresses of interfaces that could not be resolved by the HP Network Node Manager i Software.

To view the unresolved IPs of flow reporting interfaces, click **Unresolved NNM IP** in the NNM iSPI Performance for Traffic Configuration form.

The view shows the following details:

- IP address: IP address of the interface that is configured to report the traffic flow data.
- Interface index: Index of the interface.
- Last attempt time: Time-stamp of the last attempt by the NNM iSPI Performance for Traffic to resolve the IP address.

Click the  Refresh icon to refresh the list of attempts.

Listing the Undefined Applications for a Leaf Collector

When a flow record contains applications that do not satisfy any existing application mapping rule, NNM iSPI Performance for Traffic marks these applications as "Undefined Application".

NNM iSPI Performance for Traffic Undefined Applications form enables you to list and view the applications for which no application mapping exists.

If you see these Undefined Applications generating significant volume of traffic, you can create the application mappings to identify the applications contributing to traffic volume.

The Undefined Applications form lists the following parameters:

Column Name	Description
Destination Port	The port that does not have any application mapping configured
Number of Bytes	Traffic volume generated from this port
Node Name	The node for which the port is configured
Interface Name	The interface for which the port is configured
Ingress/Egress	Type of traffic generated from the port

Threshold Exceptions Reporting Nodes View

The Threshold Exceptions Reporting Nodes view presents the list of all nodes on the network that host at least one interface that breached a NNM iSPI Performance for Traffic threshold.

To open the Threshold Exceptions Reporting Nodes view:

1. In the **Workspaces** navigation pane, select the **Traffic Analysis** workspace.
2. Select the **Threshold Exceptions Reporting Nodes** view.

For each node displayed, you can see the following information:

- **Threshold State:** Threshold state for the node
The states can be Exceeded or Normal.
- **Node Name:** Hostname of the node
- **Traffic Type:** Type of traffic data passing through the node

For more details on each node, open the [Traffic Reporting Node form](#).

Analysis Pane in the Threshold Breached Reporting Nodes view

The Analysis Panel in the Threshold Breached Reporting Nodes view provides additional details on the selected node.

The Summary pane displays the analysis period for the traffic passing through the node.

The rightmost pane displays the following tabs:

- Top Apps-In:¹
- Top Apps-Out:²
- Top ToS-In:³
- Top ToS-Out:⁴
- Top IP Protocol-In:⁵
- Top IP Protocol-Out:⁶

Threshold Exceptions Reporting Interfaces View

The Threshold Exceptions Reporting Interfaces view presents the list of all interfaces on the network that breached a NNM iSPI Performance for Traffic threshold.

To open the Threshold Exceptions Reporting Interfaces view:

1. In the **Workspaces** navigation pane, select the **Traffic Analysis** workspace.
2. Select the **Threshold Exceptions Reporting Interfaces** view.

For each interface displayed, you can see the following information:

- **Threshold State:** Threshold state for the node. The states can be Exceeded or Normal.
- **Interface Name:** Qualified interface name for the interface
- **Hosted On:** Hostname of the node on which the interface is hosted
- **Traffic Type:** Type of traffic data passing through the interface
- **Flow Processing Enabled:** Shows if the interface is enabled to collect flow packets
- **Tenant Name:** Shows the name of the tenant to which the node is assigned to
- **Is Active:** Shows active and inactive flow-enabled interfaces

For more details on each interface, open the [Traffic Reporting Interface form](#).

Analysis Pane in the Threshold Breached Reporting Interfaces view

The Analysis Panel in the Threshold Exceptions Reporting Interfaces view provides additional details on the selected node.

The Summary pane displays the analysis period for the traffic passing through the interface.

¹ In this tab, a pie chart displays the top applications that are contributing to the ingress network traffic as reported by all the interfaces hosted on the node.

² In this tab, a pie chart displays the top applications that are contributing to the egress network traffic as reported by all the interfaces hosted on the node.

³ In this tab, a pie chart displays the top Type-of-Service values that are contributing to the ingress network traffic as reported by all the interfaces hosted on the node.

⁴ In this tab, a pie chart displays the top Type-of-Service values that are contributing to the egress network traffic as reported by all the interfaces hosted on the node.

⁵ In this tab, a pie chart displays the top IP protocols that are contributing to the ingress network traffic as reported by all the interfaces hosted on the node.

⁶ In this tab, a pie chart displays the top IP protocols that are contributing to the egress network traffic as reported by all the interfaces hosted on the node.

The rightmost pane displays the following tabs:

- Top Apps-In:¹
- Top Apps-Out:²
- Top ToS-In:³
- Top ToS-Out:⁴
- Top IP Protocol-In:⁵
- Top IP Protocol-Out:⁶

Incident Types Supported by NNM iSPI Performance for Traffic

NNM iSPI Performance for Traffic supports the following incident types. All the incidents have Critical severity

1. InterfaceTraffic: Signifies the following:
 - High traffic \$mtype \$metric reported through an interface \$interfaceName on the node \$nodeName.
 - Configured threshold: \$configuredValue and Measured value: \$reportedValue.
 - Measurement time is: \$reportedTime
2. InterfaceApplicationTraffic: Signifies the following:
 - High traffic \$mtype \$metric reported through an interface \$interfaceName on the node \$nodeName for the application \$application.
 - Configured threshold: \$configuredValue and Measured value: \$reportedValue.
 - Measurement time is: \$reportedTime
3. InterfaceApplicationSiteTraffic: Signifies the following:
 - High traffic \$mtype \$metric reported through an interface \$interfaceName on the node \$nodeName in site \$siteName for an application \$application.
 - Configured threshold: \$configuredValue and Measured value: \$reportedValue.
 - Measurement time is: \$reportedTime

¹ In this tab, a pie chart displays the top applications that are contributing to the ingress network traffic as reported by the interface.

² In this tab, a pie chart displays the top applications that are contributing to the egress network traffic as reported by the interface.

³ In this tab, a pie chart displays the top Type-of-Service values that are contributing to the ingress network traffic as reported by the interface.

⁴ In this tab, a pie chart displays the top Type-of-Service values that are contributing to the egress network traffic as reported by the interface.

⁵ In this tab, a pie chart displays the top IP protocols that are contributing to the ingress network traffic as reported by the interface.

⁶ In this tab, a pie chart displays the top IP protocols that are contributing to the egress network traffic as reported by the interface.

4. InterfaceSiteTraffic: Signifies the following:
 - High traffic \$mtype \$metric reported through an interface \$interfaceName on the node \$nodeName for site \$siteName.
 - Configured threshold: \$configuredValue and Measured value: \$reportedValue.
 - Measurement time is: \$reportedTime
5. InterfaceTosTraffic: Signifies the following:
 - High traffic \$mtype \$metric reported through an interface \$interfaceName on the node \$nodeName for the ToS \$tos.
 - Configured threshold: \$configuredValue and Measured value: \$reportedValue.
 - Measurement time is: \$reportedTime
6. InterfaceTosSiteTraffic: Signifies the following:
 - High traffic \$mtype \$metric reported through an interface \$interfaceName on the node \$nodeName for the ToS \$tos in site \$siteName.
 - Configured threshold: \$configuredValue and Measured value: \$reportedValue.
 - Measurement time is: \$reportedTime
7. NodeTraffic: Signifies that one or more interfaces on node: \$node has breached the traffic thresholds, where:
 - \$mtype is INGRESS or EGRESS
 - \$metric is BANDWIDTH or VOLUME
 - \$interfaceName is InterfaceName
 - \$nodeName is nodeName
 - \$configuredValue threshold condition
 - \$reportedValue value reported
 - \$reportedTime reporting time
 - \$siteName is site name
 - \$tos is tos.
 - \$app is Application

Chapter 4

NNM iSPI Performance for Traffic Maps

The NNM iSPI Performance for Traffic Maps feature enables you to view the traffic flow information of NNM iSPI Performance for Traffic enabled nodes in the network in a graphical form. NNM iSPI Performance for Traffic maps obtains information about any nodes that sends traffic flow to your network.

You can view all the top destinations and applications that contributes to the traffic flow in your network at a given point of time. The following NNM iSPI Performance for Traffic maps are available in the NNMi console:

- Destination and Application Map
- Top Sources by Destination Map
- Traffic Path View

Accessing Maps

To access the maps:

1. Select the table view you want from the Workspaces navigation panel. (For example, select the Inventory workspace, Nodes view.)
2. In the table view, click the selection box corresponding to the required node.
3. Select the **Actions** menu in the main toolbar and select **Traffic Maps**.
4. Select the required map from the list.
5. Filter the information as required.
6. Click **Get Data** in the selected map form.

Types of Maps

The NNM iSPI Performance for Traffic presents the following types of maps:

- **Destination and Application Map:** This map displays the top destinations and applications that contribute to the traffic flow to your network. If the applications are directly connected to an IP address, the IP address is considered a destination. Some destination IP addresses may be connected to multiple applications. The map is neither a network topology map nor a device centric map. It represents the logical views of traffic flows in a network. Top N means top N application plus top N destinations grouped together.
- **Top Sources by Destination Map:** This map displays the top source IP addresses that contribute to the traffic flow to a destination. You can get the information about the top contributors of traffic on your network. The map is displayed based on the IP address specified in the NNMi console. This selected IP address is considered as the source of the traffic flow. The IP address of the node from which the map is launched, should be recognized by the respective leaf collector.
This map enables you to:

- View the traffic flow heading to any destination IP address in the network. It is not necessary for the IP address to be managed by NNMi.
- Generate the logical views of traffic flowing from the Top N sources to the specified destination in a network. This map is neither a network topology map nor a device centric map.
- Display the traffic flowing from each IP address if a flow generator (router or switch) has multiple IP addresses. The colors of destination IP addresses displayed in the NNM iSPI Performance for Trafficmap are not associated with the status colors in NNMi.
- **Traffic Path View:** This map displays the flow of network traffic. Path View calculates the route that data flows between two IP addresses where NNM iSPI Performance for Traffic is enabled, and provides a map of that information. The two IP addresses can be assigned to any combination of end nodes or routers. To display meaningful information in the Path View map, make sure that you select valid IP addresses in the Source Node and Destination Node fields. This map enables you to:
 - Generate a topology map where the NNM iSPI Performance for Traffic information is overlaid on the NNMi information
 - Display the direction of the traffic flow.
 - Deduce the metric data on the inflow side based on the reported flows on the first flow exporter in the path.
 - Deduce the destination metric data by the last flow exporter on the path.
 - Query the destination host IP address in the database for IP addresses entered in the map controls and Destination Host Name for the FQDN. While accessing the Traffic Path view map, besides applying the common filters, in the Source and Destination fields, you must designate the IP addresses at both ends of the path using either the IPv4 address.

Chapter 5

Global Network Management Environment

You can deploy the NNM iSPI Performance for Traffic in the Global Network Management (GNM) setup, which consists of regional NNMi management servers and a global NNMi management server.

In a GNM setup, you can add Master and Leaf Collectors that belong to a different regional manager to your local configuration as remote collectors.

The NNM iSPI Performance for Traffic offers full support for deployment in a Global Network Management environment. Each instance has the following components:

- NNMi
- Network Performance Server
- The NNM iSPI Performance for Traffic Master Collector
- The NNM iSPI Performance for Traffic Leaf Collectors

The NNMi in the Global Manager receives data from the regional managers. The Master Collector in the global manager can be configured to receive data from the regional Master Collectors in the following ways:

- The Master Collector in the global manager can receive data from the Master Collector in the regional manager. In this case, you must add the regional Master Collector as a remote Master source in the Global Master Collector. This ensures that the complete set of data received by the regional Master Collector is forwarded to the Global Master Collector. In the above scenario, the global Master Collector receives data processed by both Traffic Leaf 1 and Traffic Leaf 2.
- The Master Collector in the global manager can receive data directly from a regional Leaf Collector system, bypassing the regional Master Collector. In this case the regional Leaf Collector (Traffic Leaf 3 in the above scenario) can be added as a leaf remote source to the global Master Collector. This ensures that the data received by all the Leaf Collectors on the remote Leaf Collector system is sent to the regional Master Collector as well as the global Master Collector. The regional Master Collector or the regional Leaf Collector can only be configured to send data to the global Traffic Master Collector. The global Master Collector cannot administer and manage these components.


Best Practice

Add all the regional Master Collectors as remote Master sources to the global Master Collector.

Add Remote Leaf Collectors

The NNM iSPI Performance for Traffic Configuration form enables you to add Leaf Collectors that belong to a different regional NNMi to your local configuration.

To add a remote Leaf Collector:


1. In the NNM iSPI Performance for Traffic Configuration form, click **Leaf Remote Sources**.
2. In the Leaf Remote Sources view, click the  Add icon. A new form opens.

3. In the new form, specify the following details:
 - Remote Leaf Hostname: Hostname of the remote Leaf Collector system.
 - Leaf Password: Password of the Leaf Collector configured during the installation of the collector.
 - JNDI Port: JNDI port of the collector.
 - HTTP Port: HTTP port of the collector.
4. Click **Save & Close**.

Edit Remote Leaf Collectors

The NNM iSPI Performance for Traffic Configuration form enables you to edit the existing remote Leaf Collectors in your configuration.


To edit a remote Leaf Collector:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Leaf Remote Sources**.
2. In the Leaf Remote Sources view, select a Leaf Collector, and then click the  Open icon. A new form opens.
3. In the new form, follow these steps:
 - Leaf password
 - JNDI port
 - HTTP port
4. Click **Save & Close**.

Add Remote Master Collectors

The NNM iSPI Performance for Traffic Configuration form enables you to add Master Collectors that belong to a different regional NNMi to your local configuration. You can use this procedure to associate all regional managers with the global manager.


To add a remote Master Collector:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Master Remote Sources**.
2. In the Master Remote Sources view, click the  Add icon. A new form opens.
3. In the new form, specify the following details:
 - Remote Master Hostname: Hostname of the remote Master Collector system.
 - Master Password: Password of the Master Collector configured during the installation of the collector.
 - JNDI Port: JNDI port of the collector.
 - HTTP Port: HTTP port of the collector.
4. Click **Save & Close**.

Edit Remote Master Collectors

The NNM iSPI Performance for Traffic Configuration form enables you to edit the existing remote Master Collectors in your configuration.

To edit a remote Master Collector:

1. In the NNM iSPI Performance for Traffic Configuration form, click **Master Remote Sources**.
2. In the Master Remote Sources view, select a Master Collector, and then click the  Open icon. A new form opens.
3. In the new form, follow these steps:
 - Master password
 - JNDI port
 - HTTP port
4. Click **Save & Close**.

Chapter 6

Accessing Details of Traffic Data Sources

Interfaces with the flow reporting capability on the network can be configured to send the traffic data to Leaf Collectors. The Leaf Collectors process and aggregate the data obtained from different devices and send the data to the Master Collector.

The NNMi console provides you with the **Traffic Analysis** workspace to monitor the availability and status of the following critical components in monitoring the network traffic:

- **Traffic Reporting Interfaces:** Interfaces on the devices that are configured to send the traffic data to Leaf Collectors.
- **Traffic Reporting Nodes:** Nodes (devices) that host the above interfaces.

These details are presented in the following views: Traffic Reporting Interfaces and Leaf Collectors. Each view lists items in a tabular format. The Analysis pane, available with each view, presents additional details on the item selected in the view.

Traffic Reporting Interfaces View

The Traffic Reporting Interfaces view presents the list of all interfaces on the network that send the traffic data to Leaf Collectors.

To open the Traffic Reporting Interfaces view:

1. In the **Workspaces** navigation pane, select the **Traffic Analysis** workspace.
2. Select the **Traffic Reporting Interfaces** view.

For each interface displayed, you can see the device name that hosts the interface, the type of traffic data the interface forwards to the Leaf Collector, and whether the device is actively sending the traffic data to the Leaf Collector or not. For more details on each interface, open the [Traffic Reporting Interface form](#).

Analysis Pane in the Traffic Reporting Interfaces view

The Analysis Panel in the Traffic Reporting Interfaces view provides additional details on the selected interface.

The Summary Pane displays the following details:

- **Traffic Interface Class:** The class name of the interface.
- **Provider Date:** The date when the data was requested from the interface for the last time
- **Total In:** Total incoming traffic (in bytes) to the interface
- **Total Out:** Total outgoing traffic (in bytes) from the interface

The rightmost pane displays the following tabs:

- **Top Apps-In:** This tab displays a pie-chart for the applications contributing to the maximum amount of the incoming traffic volume for the selected node or interface. The chart displays the

distribution of the traffic flow data for the last one hour, with each application represented by a unique color. Click on a section to view the application name and its contribution to the total volume of incoming traffic. Click on a section to view the application group name and its contribution to the total volume of incoming traffic.

- **Top Apps-Out:** This tab displays a pie-chart for the applications contributing to the maximum amount of the outgoing traffic volume for the selected node or interface. The chart displays the distribution of the traffic flow data for the last one hour, with each application represented by a unique color. Click on a section to view the application name and its contribution to the total volume of outgoing traffic. Click on a section to view the application group name and its contribution to the total volume of outgoing traffic.
- **Top ToS-In:** In this tab, a pie chart displays the top Type-of-Service values reported by the interface that are contributing to the ingress network traffic.
- **Top ToS-Out:** In this tab, a pie chart displays the top Type-of-Service values reported by the interface that are contributing to the egress network traffic.
- **Top IP Protocol-In:** In this tab, a pie chart displays the top IP protocols reported by the interface that are contributing to the ingress network traffic.
- **Top IP Protocol-Out: Top IP Protocol-In Pie Chart:** In this tab, a pie chart displays the top IP protocols reported by the interface that are contributing to the egress network traffic.
- **Performance:** The Performance tab for a selected flow enabled interface displays the following graphs for the last one day:
 - Average Utilization for the selected interface¹
 - Availability for the selected interface²
 - Interface Traffic Flows for the selected interface³
 - Traffic Volume for the selected interface⁴

These metrics may display different values in these graphs than those displayed in the NNM iSPI Performance for Traffic report graphs, due to different time grain selected for metrics summarization.

You can change the metrics and the time range for these graphs as follows:

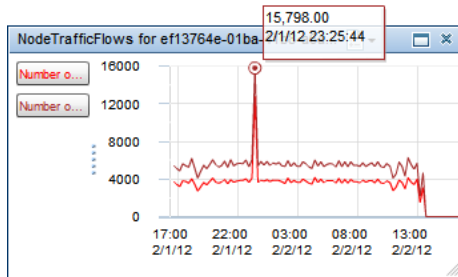
To display the metric value for a specific point of time, hover the mouse pointer on the graph.

¹Analyzes the Utilization (avg), Utilization In (avg), and Utilization Out (avg) metrics. Displayed only if NNM iSPI Performance for Metrics is installed.

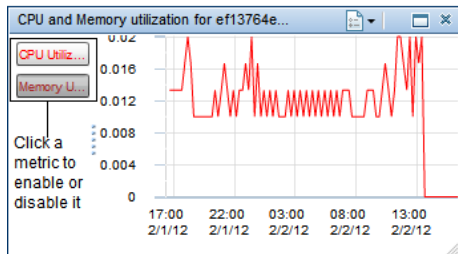
²Analyzes the Availability (avg) metric. Displayed only if NNM iSPI Performance for Metrics is installed.

³Analyzes the Number of Flows - Outgoing (sum) and Number of Flows - Incoming (sum) metrics


⁴Analyzes the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics.



To display or hide a metric, click the metric name on the legend.



To view the graph as a table, follow these steps:

- a. Click  **Options**.
- b. Select **View as Table**.

To select a date range for the graphs, follow these steps:

- a. Click **Show Date Range Panel** on the top right corner of the Performance tab.
- b. Click the graph that you want to change.

To apply the new date range on all graphs, select **All** on the Date Range panel.


- c. Select a time range for the graphs.

Traffic Reporting Interface Form

The Traffic Reporting Interface form provides details about the selected Traffic Reporting interface.

The Threshold Exceptions Reporting Interfaces view presents the list of all interfaces on the network that breached a NNM iSPI Performance for Traffic threshold. For information on the interfaces that breached a threshold, see [Threshold Exceptions Reporting Interfaces View](#).

To open a Traffic Reporting Interface form:

1. In the **Workspaces** navigation pane, select the **Traffic Analysis** workspace.
2. Select the **Traffic Reporting Interfaces** view.
3. Select an interface of your choice, and then click  **Open**.

The General pane enables you to analyze the following information for the selected flow-enabled interface:

- Interface Name: Qualified name of the interface
- Hosted on: Hostname of the system that hosts the flow reporting interface
- Traffic Type: The type of the traffic data the interface sends to the Leaf Collectors

- Flow Processing Enabled: Shows if the interface is enabled to collect flow packets
- Threshold State: Shows the threshold state for the node. The state can be Exceeded or Normal.
- Tenant Name: Shows the name of the tenant to which the node is assigned to

The Activity State pane shows the following information for the selected flow-enabled interface:

- Is Active: Shows active and inactive flow-enabled interfaces. When a flow-enabled interface does not send traffic data for a specified detection interval, the interface is shown as inactive and does not contribute to license point consumption.
- Last Flow Received At: Shows when the Leaf Collector received the last flow packet. If you restart the Master Collector, this field shows 'No flows received since Master start'. This field is automatically updated when the Master Collector receives traffic data.

The default detection interval to determine the inactive status of the flow-enabled interface is 720 minutes. When flow is detected on the inactive flow-enabled interface before the next polling starts, this interface is marked as active again in the next polling cycle. The default polling interval between the two polls is 60 minutes. You can modify these intervals as follows:

1. On the Master Collector system, go to the following directory:
On Windows
`%nmdatadir%\nmsas\traffic-master\conf`
On Linux
`/var/opt/OV/nmsas/traffic-master/conf`
2. Use a text editor to open the `nms-traffic-master.address.properties` file.
3. Set the `inactive-flow.detection.interval` property to a required value (in minutes) of the detection interval that determines the inactive status of the flow-enabled interface.
4. Set the `inactive-flow.detector.thread.wake-up.interval` property to a required value (in minutes) of polling interval. Reducing this time interval significantly might impact the performance of the Master Collector. You can reduce the polling interval to minimum value of 1 minute.
5. Save and close the file.

The right pane shows the following details for ingress and egress flows collected by the interface:

- Top 5 Sources
- Top 5 Destinations
- Top 5 Conversations
- Applicable Threshold
- Incidents

Click , and then click **Open** to open the Interface form for the selected interface.

The Analysis pane displays additional details on the selected interface. For more information about Analysis pane, see [Traffic Reporting Interfaces View](#).

Traffic Reporting Nodes View

The Traffic Reporting Nodes view presents the list of all nodes on the network that host flow collector interfaces that are capable of sending the traffic data to Leaf Collectors.

To open the Traffic Reporting Nodes view:

1. In the **Workspaces** navigation pane, select the **Traffic Analysis** workspace.
2. Select the **Traffic Reporting Nodes** view.

For each node displayed, you can see the hostname of the node and the type of traffic data the interface (which is hosted on the node) forwards to the Leaf Collector. For more details on each node, open the Traffic Node form.

Analysis Pane in the Traffic Reporting Nodes view

The Analysis Pane in the Traffic Reporting Nodes view provides additional details on the selected node.

The Summary Panel displays the analysis period for the traffic reporting interface hosted on the node.

The rightmost pane displays the following tabs:

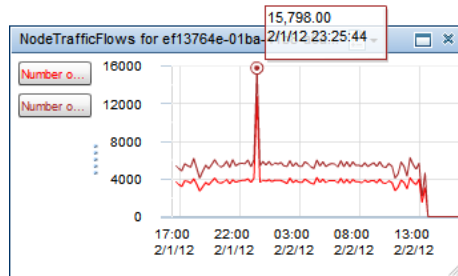
- **Top Apps-In:** This tab displays a pie-chart for the applications contributing to the maximum amount of the incoming traffic volume for the selected node or interface. The chart displays the distribution of the traffic flow data for the last one hour, with each application represented by a unique color. Click on a section to view the application name and it's contribution to the total volume of incoming traffic. Click on a section to view the application group name and it's contribution to the total volume of incoming traffic.
- **Top Apps-Out Pie Chart:** This tab displays a pie-chart for the applications contributing to the maximum amount of the outgoing traffic volume for the selected node or interface. The chart displays the distribution of the traffic flow data for the last one hour, with each application represented by a unique color. Click on a section to view the application name and it's contribution to the total volume of outgoing traffic. Click on a section to view the application group name and it's contribution to the total volume of outgoing traffic.
- **Top ToS-In Pie Chart:** In this tab, a pie chart displays the top Type-of-Service values that are contributing to the ingress network traffic as reported by all the interfaces hosted on the node.
- **Top ToS-Out Pie Chart:** In this tab, a pie chart displays the top Type-of-Service values that are contributing to the egress network traffic as reported by all the interfaces hosted on the node.
- **Top IP Protocol-In Pie Chart:** In this tab, a pie chart displays the top IP protocols that are contributing to the ingress network traffic as reported by all the interfaces hosted on the node.
- **Top IP Protocol-Out Pie Chart:** : **Top IP Protocol-In Pie Chart:** In this tab, a pie chart displays the top IP protocols that are contributing to the egress network traffic as reported by all the interfaces hosted on the node.
- **Performance:** The Performance tab for a selected flow enabled interface displays the following graphs for the last one day:

- CPU and Memory Utilization for the selected node¹
- CPU and Memory Exception Rate for the selected node²
- Interface Traffic Flows for the selected node³
- Traffic Volume for the selected node⁴

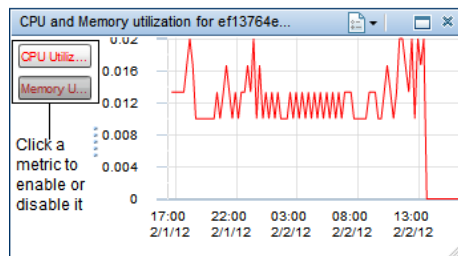
These metrics may display different values in these graphs than those displayed in the NNM iSPI Performance for Traffic report graphs, due to different time grain selected for metrics summarization.

You can change the metrics and the time range for these graphs as follows:


To display the metric value for a specific point of time, hover the mouse pointer on the graph.



To display or hide a metric, click the metric name on the legend.



To view the graph as a table, follow these steps:

- a. Click  **Options**.
- b. Select **View as Table**.

To select a date range for the graphs, follow these steps:

¹Analyzes the Memory Utilization (avg) and CPU Utilization (avg) metrics. Displayed only if NNM iSPI Performance for Metrics is installed.

²Analyzes the CPU Utilization - Threshold Exception Rate (avg) and Memory Utilization - Threshold Exception Rate (avg) metrics. Displayed only if NNM iSPI Performance for Metrics is installed.

³Analyzes the Node Traffic Flows for the selected node - Outgoing (sum) and Node Traffic Flows for the selected node - Incoming (sum) metrics

⁴ NNM iSPI Performance for Traffic displays this graph only if the node exports Netflow (versions 5 or 9), SFlow version 5, or IPFIX traffic data. This graph analyzes the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics.


- a. Click **Show Date Range Panel** on the top right corner of the Performance tab.
- b. Click the graph that you want to change.
To apply the new date range on all graphs, select **All** on the Date Range panel.
- c. Select a time range for the graphs.

Traffic Node Form

The Traffic Node form provides details about the selected Traffic Reporting node.

The Threshold Exceptions Reporting Nodes view presents the list of all nodes on the network that host at least one interface that breached a NNM iSPI Performance for Traffic threshold. For information on the nodes that breached a threshold, see [Threshold Exceptions Reporting Nodes View](#).

To open a Traffic Node form:


1. In the **Workspaces** navigation pane, select the **Traffic Analysis** workspace.
2. Select the **Traffic Reporting Nodes** view.
3. Select a node of your choice, and then click  **Open**.

The General pane of the form enables you to analyze the following information for the selected node:

- **Node Name:** Name of the node
- **Traffic Type:** The type of the traffic data that the node handles

The right pane shows the following details for ingress and egress flows collected by the interface:

- Top 5 Sources
- Top 5 Destinations
- Top 5 Conversations
- Traffic Reporting Interfaces
- Applicable Threshold
- Incidents

To view operational details of the interface (and the device that hosts the interface), click , and then click **Open**.

The Analysis pane displays additional details on the selected node. For more information about Analysis pane, see [Traffic Reporting Nodes View](#).

Disabling Interfaces to Report Flow Data

You can configure the NNM iSPI Performance for Traffic to stop processing flows from select interfaces. As a result, flows reported by the selected interfaces are not analyzed and those flows do not contribute to the reports. The NNM iSPI Performance for Traffic provides you with a command line utility to perform this configuration.

To configure the NNM iSPI Performance for Traffic to stop processing flows:

1. Log on to the Master Collector system with the root or administrator privileges.
2. Go to the following directory:
On Windows
`<Master_Install_Dir>\nonOV\traffic-master\bin`
On Linux
`/opt/OV/nonOV/traffic-master/bin`
3. Run the following command:
nmstrafficdisableflow.ovpl -u system -p <system_user_password> -i <Interface_UUID>
In this instance,
`<system_user_password>` is the password for the Master Collector system user (created during the installation).
`<Interface_UUID>` is the UUID of the flow reporting interface that you want to exclude.

The status of the interface in the Flow Reporting Interfaces view appears as `Disabled`. As a result, the license consumption of the NNM iSPI Performance for Traffic is also reduced accordingly. For example, if you stop processing flows from a NetFlow interface, the license consumption of the NNM iSPI Performance for Traffic gets reduced by five iSPI points.

Tip: To find the UUID of an interface, go to the Interfaces View (inventory) in the NNMi console, select the interface and open the Interface form, and then go to the Registration tab. The UUID of the interface is displayed in the Registration tab.

To include the flows from the interface again, run the following command:


nmstrafficenableflow.ovpl -u system -p <system_user_password> -i <Interface_UUID>

NNM iSPI Performance for Traffic Leaf Collectors

The NNM iSPI Performance for Traffic Leaf Collectors view displays a list of the existing Leaf Collector instances.

Using this form, you can view properties and performance of the collector instances available in your NNM iSPI Performance for Traffic deployment.

To open the NNM iSPI Performance for Traffic Leaf Collectors view:

1. In the Workspaces navigation pane, select the **Configuration** workspace.
2. Select the **NNM iSPI Performance for Traffic Leaf Collectors** view.
3. Select the Leaf Collector instance that you want to view.
4. Click the  Open icon. For each leaf collector displayed, you can view the following information:
 - General Information
 - [Collector Statistics History](#)
 - [Flow Processing Status](#)

Viewing Collector Statistics History

You can view the list of activities performed by a Leaf Collector from the NNM iSPI Performance for Traffic Leaf Collectors view.

To view Leaf Collector statistics:

1. In the NNM iSPI Performance for Traffic Leaf Collectors view, double-click a collector. The Leaf Collector form opens.
2. In the Leaf Collector form, go to the Collector Statistics History tab, and then double-click an entry. The Collector Statistics History form opens.

The Collector Statistics History tab shows the following details:

- Last Flush Time
- Number of Flows
- Number of Flushed
- Number of Packets

Viewing Flow Processing Status

You can view the history of flow records processed by a Leaf Collector from the NNM iSPI Performance for Traffic Leaf Collectors view.

To view flow processing status:

1. In the NNM iSPI Performance for Traffic Leaf Collectors view, double-click a collector. The Leaf Collector form opens.
2. In the Leaf Collector form, go to the Flow Processing Status tab, and then double-click an entry. The Flow Processing Status form opens.

The Flow Processing Status tab shows the following details:

- Open Time: ¹
- Closed Time: ²
- Status: ³
- Message: ⁴
- Suggested Solution: ⁵

¹Displays the starting time for the flow processing

²Displays the time when the flow processing was stopped

³Displays the status of the flow

⁴Displays the reason or problem for which the flow processing stopped

⁵Displays the suggested solution to resolve the problem

Site Inventory Analysis Using the Traffic Sites View

Using the Traffic Sites view, you can view the list of the **site**¹s created in your environment.

The sites inherit the security features set for the flow reporting interfaces. You can assign nodes to Tenant and Security Group settings using NNMi. The flow reporting interfaces inherits these Tenant and Security Group settings from the associated nodes.

To open the Traffic Sites view:

1. In the **Workspaces** navigation pane, select the **Traffic Analysis** workspace.
2. Select the **Traffic Sites** view.

For each site displayed, you can see the site name, **site priority**², site description, and the tenant name for the site.

Analysis Pane in the Traffic Reporting Interfaces view

The Analysis panel displays the following attributes of the selected site:

Pane Name	Pane Description
Site Summary	The Site Summary pane displays the following information: <ul style="list-style-type: none">• Current Time• Analysis period for the selected site
Source Site - Top Apps - In	Displays the top five applications that generate the maximum volume of incoming (ingress) traffic for the last one hour. Considers only the traffic flow records generated from the selected site.

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


²An interface can be associated to only one site. While creating the site, you need to specify an ordering number for the site to resolve conflicts in case an interface matches multiple sites. The NNM iSPI Performance for Traffic associates the interfaces 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 Traffic assigns default ordering. Default ordering for a site is given the lowest priority. If an interface matches multiple sites, the site with the lower ordering gains priority to associate with the interface.

Source Site - Top Apps - Out	Displays the top five applications that generate the maximum volume of outgoing (egress) traffic for the last one hour. Considers only the traffic flow records generated from the selected site.
Destination Site - Top Apps - In	Displays the top five applications that generate the maximum volume of incoming (ingress) traffic for the last one hour. Considers only the traffic flow records flowing towards the selected site.
Destination Site - Top Apps - Out	Displays the top five applications that generate the maximum volume of outgoing (egress) traffic for the last one hour. Considers only the traffic flow records flowing towards the selected site.
Source Site - Top ToS - In	Displays the top five classes of service that generate the maximum volume of incoming (ingress) traffic for the last one hour. Considers only the traffic flow records generated from the selected site.
Source Site - Top ToS - Out	Displays the top five classes of service that generate the maximum volume of outgoing (egress) traffic for the last one hour. Considers only the traffic flow records generated from the selected site.
Destination Site - Top ToS - In	Displays the top five classes of service that generate the maximum volume of incoming (ingress) traffic for the last one hour. Considers only the traffic flow records flowing towards the selected site.
Destination Site - Top ToS - Out	Displays the top five classes of service that generate the maximum volume of outgoing (egress) traffic for the last one hour. Considers only the traffic flow records flowing towards the selected site.

Traffic Site Form

The Traffic Site form provides details about the selected Traffic site.

To open a Traffic Site form:

1. In the **Workspaces** navigation pane, select the **Traffic Analysis** workspace.
2. Select the **Traffic Sites** view.
3. Select a site of your choice, and then click  **Open**.

The General pane of the form enables you to analyze the following information for the selected site:

- Site Name
- **Site Priority**¹
- Tenant Name
- Site Description

The right pane shows the following details for the nodes associated to the site:

- Traffic Reporting Nodes
- Applicable Thresholds

The Analysis panel displays additional details on the selected site. For more information about Analysis pane, see [Traffic Sites View](#).

¹An interface can be associated to only one site. While creating the site, you need to specify an ordering number for the site to resolve conflicts in case an interface matches multiple sites. The NNM iSPI Performance for Traffic associates the interfaces 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 Traffic assigns default ordering. Default ordering for a site is given the lowest priority. If an interface matches multiple sites, the site with the lower ordering gains priority to associate with the interface.

Chapter 7

Storing and Analyzing Flow Packets

The NNM iSPI Performance for Traffic provides you with a mechanism to store and analyze raw flow packets obtained from different sources by the Leaf Collector. While adding a new Leaf Collector, you can specify if you want to collect raw flow packets. After the NNM iSPI Performance for Traffic stores the flow packets on the Leaf Collector system, you can use the `nmstrafficinspectiontool.ovpl` utility to analyze the flow packets.

When you add a new Leaf Collector instance or edit an existing Leaf Collector instance, select **true** for the Store Flow in File field. The Leaf Collector stores the received flow packets into the following directory:

- *On Windows*
`<Data_Dir>\shared\traffic-leaf\data\<<Leaf_Collector_Instance>\<IP_Address_of_Source>`
- *On Linux*
`/var/opt/OV/shared/traffic-leaf/data/<Leaf_Collector_Instance>/<IP_Address_of_Source>`

Tip: Use this feature only for troubleshooting. This option has a significant impact the performance of the Leaf Collector.

For more information about adding or editing Leaf Collector instance, see [Add a Leaf Collector Instance](#) and [Edit a Leaf Collector Instance](#).


In this instance:

`<Data_Dir>`: Data directory that you chose during the installation of the Leaf Collector.

`<Leaf_Collector_Instance>`: Name of the Leaf Collector instance

`<IP_Address_of_Source>`: IP address of the device where the flow packet originated.

To disable the mechanism to store flow packets:

1. Go to the Leaf Collector view.
2. Select the Leaf Collector instance for which you want to disable the flow packet storing mechanism.
3. Click  **Open**. A new form opens.
4. In the new form, set Store Flow in File to **false**.
5. To remove the existing flow packet files, remove the `*.flow` files from the following directory:
 - *On Windows*
`<Data_Dir>\shared\traffic-leaf\data\<<Leaf_Collector_Instance>\<IP_Address_of_Source>`

- *On Linux*
/var/opt/OV/shared/traffic-leaf/data/<Leaf_Collector_Instance>/<IP_Address_of_Source>

Do not delete the directories; delete only the *.flow files. If you delete the directory, the Leaf Collector fails to store flow packets when you enable the storing mechanism again.

In this instance:

<Data_Dir>: Data directory that you chose during the installation of the Leaf Collector.

<Leaf_Collector_Instance>: Name of the Leaf Collector instance

<IP_Address_of_Source>: IP address of the device where the flow packet originated.

Analyze Flow Packets

The `nmstrafficinspectiontool.ovpl` utility enables you to view and analyze the flow packets (*.flow files) that are stored in the following directory:

- *On Windows*
<Data_Dir>\shared\traffic-leaf\data\<Leaf_Collector_Instance>\<IP_Address_of_Source>
- *On Linux*
/var/opt/OV/shared/traffic-leaf/data/<Leaf_Collector_Instance>/<IP_Address_of_Source>

The raw flow packets are saved by the Leaf Collector with the following file name format:

<IP_Address_of_Source>_<Date>_<Time>_<FlowType>_<Leaf_Collector_Instance>.flow

In this instance:

<Data_Dir>: Data directory that you chose during the installation of the Leaf Collector.

<Leaf_Collector_Instance>: Name of the Leaf Collector instance

<IP_Address_of_Source>: IP address of the device where the flow packet originated.

<Time>: The time (in the *hour_minute* format) when the collector starts storing the flow packet on the system.

<FlowType>: The type of the flow packet. Possible values are NetFlowV5, NetFlowV9, sFlow, IPFIX, and JFlow.

<Leaf_Collector_Instance>: Name of the Leaf Collector instance that receives the packet.

For example: 172.16.10.5_21-May-2010_11-20_NetflowV5_collector125.flow

To view stored flow packets:

1. Log on to the Leaf Collector system with the root (Linux) or administrator (Windows) privileges.
2. Go to the following directory:
 - *On Windows:* <Data_Dir>\shared\traffic-leaf\data\<Leaf_Collector_Instance>\<IP_Address_of_Source>
 - *On Linux:* /var/opt/OV/shared/traffic-leaf/data/<Leaf_Collector_Instance>/<IP_Address_of_Source>

3. To view the contents of all the flow packet files stored by the Leaf Collector, run the following command:

nmstrafficinspectiontool.ovpl

The contents of all the flow packet files appear in the command line console.

4. In addition to viewing the contents of all the flow packet files available in the directory, you can perform the following operations:

- **Filter the output.**

You can filter out the contents of flow packets that not of your interest by using the `-filter` option.

To filter out flow packets, run the following command:

nmstrafficinspectiontool.ovpl -filter<filter_condition>, <filter_condition>,...

In this instance, <filter_condition> is the filter condition created with one of the attributes of flow packets. The command shows the contents of the flow packets that match the filter condition. For example, the command **nmstrafficinspectiontool.ovpl -filter SrcIP 172.17.10.*** shows the contents of the flow packets that originated from systems with the IP address

- **View select attributes.**

To view only select attributes of packet files, run the following command:

nmstrafficinspectiontool.ovpl hc<attribute_name>, <attribute_name>,...

In this instance, <attribute_name> is the name of the attribute that you want to hide.

- **View a single file.**

To view the contents of a particular file, run the following command:

nmstrafficinspectiontool.ovpl -f <FlowPacketFileName>

In this instance, <FlowPacketFileName> is the name of the flow packet file (* .flow file).

The contents of the file appear in the command line console.

- **Export the contents of packet files to CSV files.**

To export the contents of the files into a CSV file, run the following command:

nmstrafficinspectiontool.ovpl -csv -csvdir <directory> **-csvname** <filename>

In this instance:

<directory> is the directory on the Leaf Collector system where the CSV file is saved.

<filename> is the file name with which the Leaf Collector saves the CSV file.

- **Export the contents of a particular file to a CSV file.**

To export the contents of a particular file to a CSV file, run the following command:

nmstrafficinspectiontool.ovpl -f <FlowPacketFileName> **-csv -csvdir** <directory> **-csvname** <filename>

In this instance:

<FlowPacketFileName> is the name of the flow packet file (* .flow file).

<directory> is the directory on the Leaf Collector system where the CSV file is saved.

<filename> is the file name with which the Leaf Collector saves the CSV file.

- **Export filtered contents to a CSV files.**

You can combine the `-csv` and `-filter` options to export filtered content to a CSV file.

To export filtered content to a CSV file, run the following command:

nmstrafficinspectiontool.ovpl -filter<filter_condition>, <filter_condition>,... **-csv -csvdir** <directory> **-csvname** <filename>

In this instance:

<filter_condition> is the filter condition created with one of the attributes of flow packets.

The command shows the contents of the flow packets that match the filter condition.
<directory> is the directory on the Leaf Collector system where the CSV file is saved.
<filename> is the file name with which the Leaf Collector saves the CSV file.

For more information on the `nmstrafficinspectiontool.ovpl` command, see reference pages.

Contents of the Flow Packet Files

A flow packet file includes the following pieces of information in its content:

- Router: The router or switch that sent the flow packet to the Leaf Collector.
- SrcIP: IP address of the system where the IP flow originated.
- DstIP: IP address of the destination system of the IP flow.
- IPProtocol: IP protocol used by the flow.
- NFSNMPInputIndex: SNMP index of the egress interface.
- NFSNMPOutputIndex: SNMP index of the ingress interface.
- SrcPort: Egress port.
- DstPort: Ingress port.
- TCPFlags: TCP flag of the traffic flow.
- IPToS: Type of Service property of the traffic flow.
- NumPacket: Number of packets in the traffic flow.
- NumBytes64: Number of bytes in the traffic flow.
- StartTime: Time when the traffic flow originated from the source system.
- EndTime: Time when the traffic flow arrived on the destination system.

Limiting the Number of the Flow Packet Files

Once configured, the Leaf Collector continues to create flow packet files on the system, which eventually consume a significant amount of disk space. When the available disk space of the Leaf Collector system falls to 10%, the Leaf Collector automatically stops creating any new flow packet files. In addition, the NNM iSPI Performance for Traffic provides you with a mechanism to control the maximum number of flow packet files on the system.

To limit the number of flow packet files:

1. Log on to the Leaf Collector system.
2. Go to the following location:
 - *On Windows:*
<DataDir>\shared\traffic-leaf\conf
In this instance, <DataDir> is the directory where you chose to place the data files while installing the Leaf Collector.
 - *On Linux:*
/var/opt/OV/shared/traffic-leaf/conf
3. Open the `nms-traffic-leaf.address.properties` file with a text editor.

4. Set the `max.dump.hours` property to the number of hours for which you want to store the flow packet files.
5. Save the file.
6. Enable the packet file storing mechanism.
After creating a flow packet file, the Leaf Collector retains the file for the number of hours specified for the `max.dump.hours` property.
For example, if you set the `max.dump.hours` property to 1, the Leaf Collector instance retains a flow packet file only for 1 hour after its creation.

