

HP Network Node Manager iSPI Performance for Traffic

Software Version: 9.20

Deployment by Example



Table of Contents

Introduction	2
Assumptions	2
Installation	3
Installing the HP NNMi Extension for iSPI Performance for Traffic	3
Installing the Master Collector	5
Installing the Leaf Collector	7
Applying Licenses	9
Getting Started	10
Launching the NNM iSPI Performance for Traffic Configuration Form	10
Validating Installation	10
Configuring the Leaf Collector	12
Configure the Leaf Collector System	12
Configure Collectors	13
Validate Data Collection by the Leaf Collector	16
Configuring User-Defined Application Mapping	20
Configuring ToS Groups	25
Configuring Sites	27
Configuring Thresholds	28
Common Use Cases	33

Introduction

This document describes the HP Network Node Manager iSPI Performance for Traffic (NNM iSPI Performance for Traffic) deployment in a small test lab setup. All the steps and snapshots given below are for the version 9.20 of the NNM iSPI Performance for Traffic. This test exercise is done on a Linux (Red Hat Enterprise Linux 5.8) system; however, Windows-equivalent path details are listed. This example deployment uses the PostgreSQL database.

Key steps in this deployment are:

1. Installation of the NNM iSPI Performance for Traffic
2. Applying a license
3. Getting started
4. Configuring the NNM iSPI Performance for Traffic Leaf Component
5. Configuring The NNM iSPI Performance for Traffic Master Component
6. Configuring User-defined Application mapping
7. Configuring Type Of Service Groups
8. Configuring sites and thresholds

This document does not cover:

- Upgrade of The NNM iSPI Performance for Traffic from older version to 9.20
- Configuring HA
- The NNM iSPI Performance for Traffic running with Oracle database
- Configuring GNM

NOTE: For details on these topics, see the *NNM iSPI Performance for Traffic Installation Guide* and *NNM iSPI Performance for Traffic Deployment Guide*.

Assumptions

- NNMi is installed and running
- The Network Performance Server (NPS) is installed and running
- You have gone through the *NNM iSPI Performance for Traffic 9.20 Installation Guide*, *Release Notes*, and *Support Matrix* documents prior to following this document
- You have gone through the first 3 chapters of the *NNM iSPI Performance for Traffic 9.20 Deployment Guide* prior to following this document

Installation

You must always use the following order of installation:

1. Install the HP NNMi Extension for iSPI Performance for Traffic on the NNMi management server.
2. Install the NNM iSPI Performance for Traffic Master Collector.
3. Install the NNM iSPI Performance for Traffic Leaf Collector.

The Master and Leaf Collectors can both be installed on the NNMi management server, or they can exist on a separate server as well. Leaf and Master support running as standalone components on different servers as well.

Best practice: In a Medium or Large scale deployment, it is recommended to have Traffic master installed on the dedicated box or on the same box as NNMi server. However, it is not recommended to have both Traffic master and NPS installed on the same server for a medium or large setup given that both the applications are resource intensive applications.

Refer to the deployment guide for more information about best practices in different deployment scenarios.

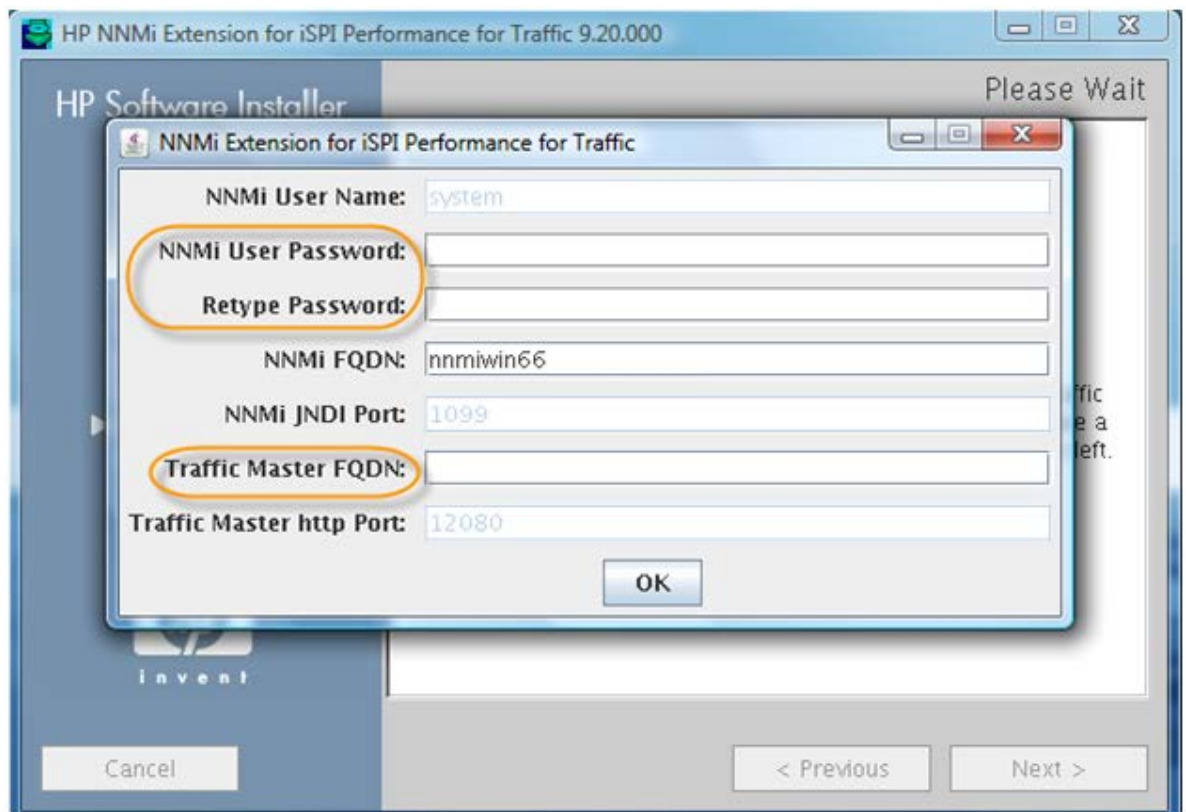
Installing the HP NNMi Extension for iSPI Performance for Traffic

This is the first component that must be installed. It must be installed on the NNMi management server. This component enables the integration of NNMi with the NNM iSPI Performance for Traffic by:

- Enabling the launch point of NNM iSPI Performance for Traffic workspace and reports from the NNMi console
- Providing NNM iSPI Performance for Traffic-specific views (Inventory, Form, Analysis Panels, Maps) in the NNMi console

You will be prompted to specify the following during the installation of this component:

- NNMi 'system' user password
- NNM iSPI Performance for Traffic Master server's fully qualified domain name (FQDN) (the FQDN of the server on which the Master Collector will be installed)

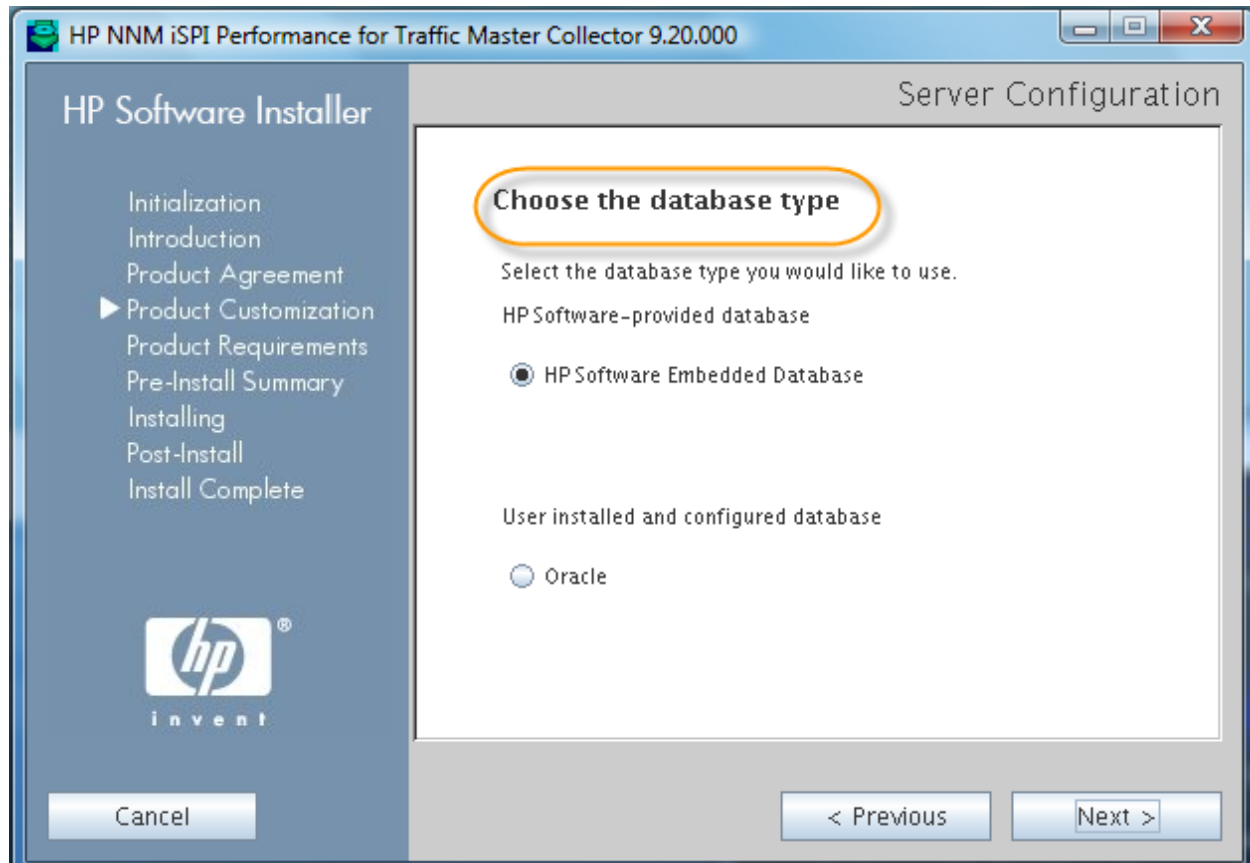


Re-start NNMi services once this component is successfully installed.

Installing the Master Collector

The Master Collector can be installed on the NNMi management server or on the different server. The Master Collector and NNMi must use the same database type. For example, if NNMi is running with the embedded database, the Master Collector must also be configured to run with the embedded database only.

When installed on a separate server from NNMi, the Master Collector installs its own instance of the embedded database.



During the installation, you will be prompted to specify:

- Web Service Client username and password using which the Master Collector will communicate with NNMi. This Web Service Client user must be created using the NNMi.

Caution: DO NOT use the NNMi 'system' user and its password here. If you have multiple iSPIs running in this setup, each iSPI must have its own Web Service Client user created in NNMi.

- You will be asked to type the NNM iSPI Performance for Traffic password. You can type a password of your choice. HP recommends that you chose the same password as that of the NNMi 'system' user.
- Select the "isSecure" checkbox if you have made the same selection for NNMi. Combination is not recommended.

If NNMi is configured for Application Failover, select the NNMi Failover Configured checkbox on the installation wizard and type the configuration details for secondary NNMi server as well.

The 'Configuring Master' window is divided into three main sections. The 'Primary NNMi Server' section on the left includes fields for FQDN, HTTP/HTTPS ports, JNDI port, and Web Service Client credentials. The 'Secondary NNMi Server' section on the right has identical fields. The 'Traffic iSPI Server' section at the bottom left includes FQDN, HTTP/HTTPS ports, and JNDI port. A 'Traffic User Name' and 'Traffic Password' are also specified. Checkboxes for 'Is Secure?' and 'NNMi Failover Configured?' are present. The 'Perf SPI Data Path' is set to a default value. 'Submit' and 'Clear' buttons are at the bottom.

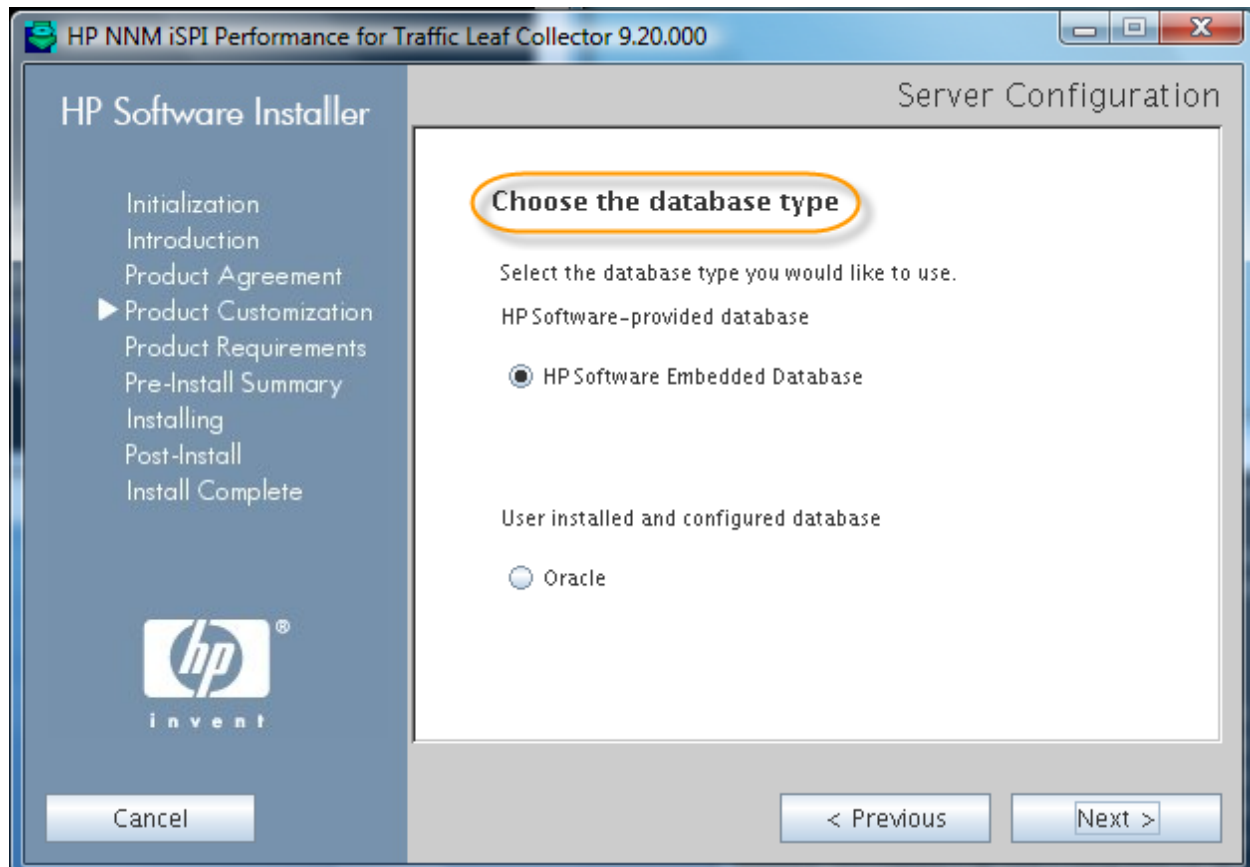
When prompted, type the FQDN of the server on which NPS is installed.

The 'Performance SPI Server Configuration' dialog box is overlaid on the main window. It contains two sections. The first section, 'HP NNM iSPI Performance Server', has fields for 'HostName' and 'Port Number' (set to 9303). The second section, 'HP NNM iSPI Performance Database Configuration', includes a checkbox 'Edit if the default UserName and Password has been modified.' and fields for 'User name' (DBA), 'Password', and 'Retype Password'. An 'Ok' button is at the bottom. The background window shows 'HP NNM iSPI Performance for Traffic Master Collector 9.20.000' with 'Cancel', '< Previous', and 'Next >' buttons.

Caution: DO NOT change the "Port Number" value give on the installation wizard from 9303 to any other port. This port is used internally by the Master Collector to communicate with the NPS database.

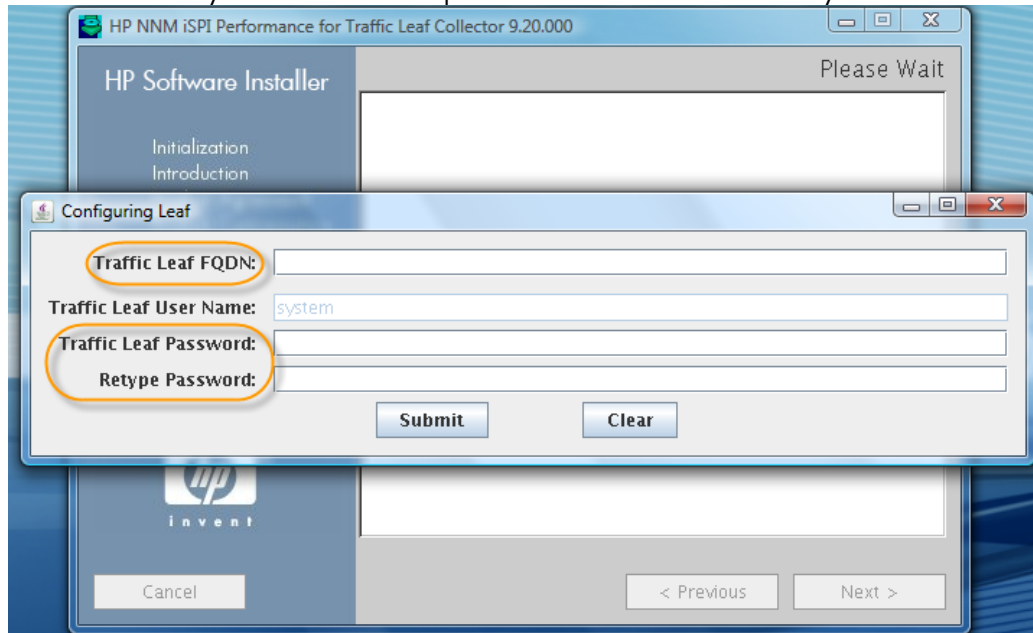
Installing the Leaf Collector

The Leaf Collector can be installed on the NNMi management server or on a dedicated server. Typically, it is installed in the subnet from which routers forwarding netflow traffic to the Leaf Collector. The Leaf Collector and NNMi must use the same database type.



When prompted, specify the FQDN of the server on which the Leaf Collector is going to be installed

You will be asked to type the Leaf Collector password. You can type a password of your choice. HP recommends that you chose the same password as that of the NNMi 'system' user.



Once installed, the administration (stop/start) of the NNM iSPI Performance for Traffic can be done as follows:

1. At the end of successful installation of each Leaf Collecto, start the traffic leaf process by running:
 %NnmInstallDir%/traffic-leaf/bin/nmstrafficleafstart.ovpl (Windows)
 \$NnmInstallDir/traffic-leaf/bin/nmstrafficleafstart.ovpl (Linux)
2. While the Master Collector runs as a standalone (not on the NNMi management server) component on a Windows system, before starting the Master Collector for the first time after installation, run the nmstrafficmastersetuser.ovpl command to set the Windows user with which Master Collector should start.
 - a) See the *NNM iSPI Performance for Traffic Installation Guide* for more details on how to create the master user.

Other process administration commands include:

- To check the status of the Master Collector process (to be run on the Master Collector system):
 - \$NnmInstallDir/traffic-master/bin/nmstrafficmasterstatus.ovpl (Linux)
 - %NnmInstallDir%/traffic-master/bin/nmstrafficmasterstatus.ovpl (Windows)
- To stop the Master Collector process (to be run on the Master Collector system):
 - \$NnmInstallDir/traffic-master/bin/nmstrafficmasterstop.ovpl (Linux)
 - %NnmInstallDir%/traffic-master/bin/nmstrafficmasterstop.ovpl (Windows)
- To check the status of the Leaf Collector process (to be run on Leaf Collector system):
 - \$NnmInstallDir/traffic-leaf/bin/nmstrafficleafstatus.ovpl (Linux)

- %NnmInstallDir%/traffic-leaf/bin/nmstrafficleafstatus.ovpl (Windows)
- To stop traffic master process (to be run on Traffic leaf server),
 - \$NnmInstallDir/traffic-leaf/bin/nmstrafficleafstop.ovpl (Unix)
 - %NnmInstallDir%/traffic-leaf/bin/nmstrafficleafstop.ovpl (Windows)
- trafficextversion.ovpl (on the NNMi management server), trafficleafversion.ovpl (on the Master Collector system), and trafficmasterversion.ovpl (on the Leaf Collector system) commands show the version and patch numbers of the installed NNM iSPI Performance for Traffic component.

This tool can be located at:

%NnmInstallDir%\traffic-leaf\bin – On the Leaf Collector system

%NnmInstallDir%\traffic-master\bin – On the Master Collector system

%NnmInstallDir%\bin - On the NNMi management server

Applying Licenses

The NNM iSPI Performance for Traffic comes with 60-day Instant-On license, but it is recommended that you apply the permanent license as soon as the iSPI is installed and running. The NNM iSPI Performance for Traffic works on the iSPI Points license. The points license has to be applied on the NNMi management server and aligned to the NNMi server IP address only.

To apply the license, run the following command on the NNMi management server:

nnmlicense.ovpl iSPI-Points -f *<License file>*

The NNM iSPI Performance for Traffic also requires the Traffic Collector Connection license when the Leaf Collector is installed on a different server from the Master Collector.

This license should also be aligned to NNMi server IP address and must be applied on the NNMi management server only. One license is required for each connection from the Leaf Collector to the Master Collector when they both are not installed on the same server.

To apply the license, run the following command on the NNMi management server:

nnmlicense.ovpl TRAFFICCOLLCON -f *<License file>*

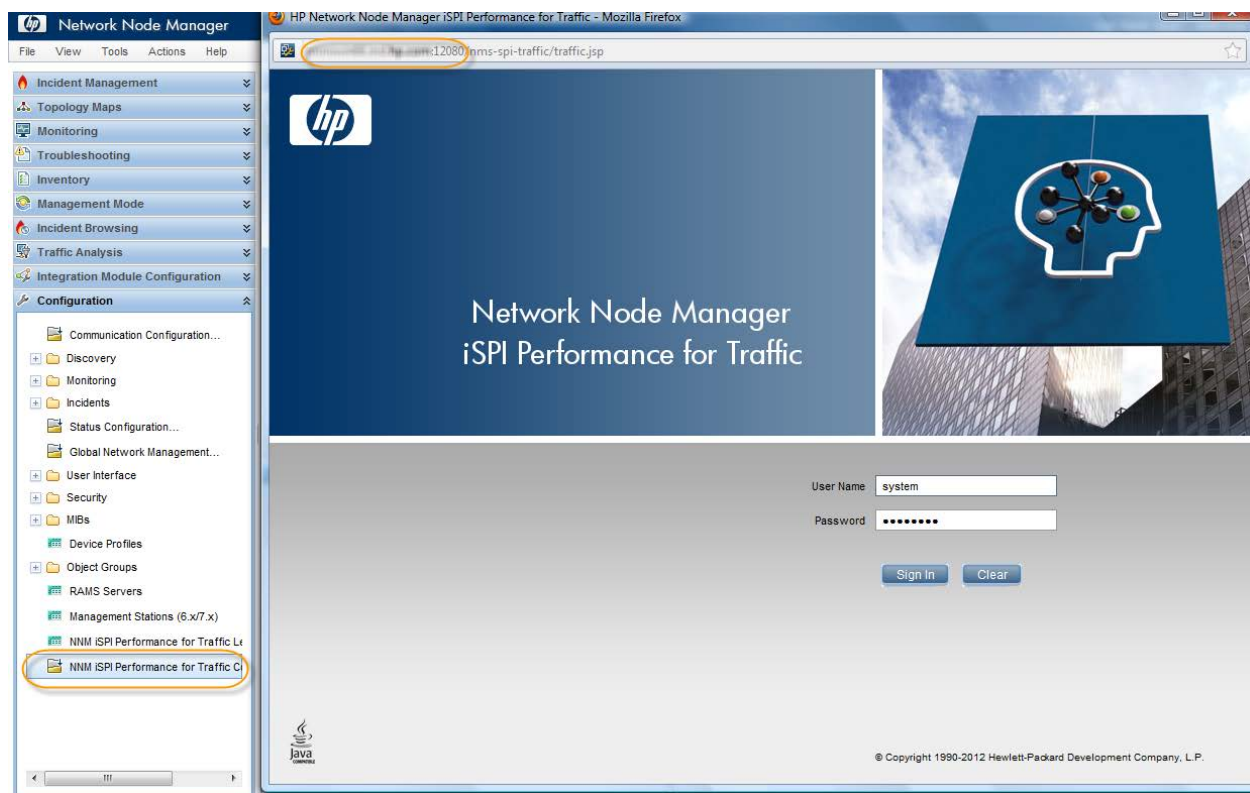
Getting Started

Tip: Make sure routers are configured to export the flow records to the Traffic Leaf system and also these routers are seeded in NNMi discovered topology.

Launching the NNM iSPI Performance for Traffic Configuration Form

You can launch the NNM iSPI Performance for Traffic Configuration form from the NNMi console.

Single Sign-On (SSO) must be enabled explicitly for the NNM iSPI Performance for Traffic Master Collector from NNMi. Without that, you can log on only with the 'system' user password that you typed during the Master Collector installation. See the "Configuring Single Sign-On (SSO)" section in the NNM iSPI Performance for Traffic deployment guide for more details.



Note that the URL being launched is on the server on which the Master Collector is installed

Validating Installation

Once the installation is successful, it is recommended that you validate the installation to ensure correct values for parameters like Leaf FQDN, Master FQDN, NPS system name, and the *PerfSPI* data directory.

To validate the installation, log on to the NNM iSPI Performance for Traffic configuration form as shown above and click **Installation Verification** in the left pane. In the right pane, you can see the values entered for configuration items during the installation. Click **Validate** to verify that the values of the configuration items are correct.

	Title	Description	Value
Primary-NNM	com.hp.ov.nms.spi.traffic-master.Nnm.https.port	The HTTPS port used by the NNMi management server	443
	com.hp.ov.nms.spi.traffic-master.Nnm.password	The administrator password for NNMi	traffic
	com.hp.ov.nms.spi.traffic-master.Nnm.username	The administrator username for NNMi	traffic
	com.hp.ov.nms.spi.traffic-master.Nnm.hostname	The fully Qualified Domain Name (FQDN) for the NNMi management server	nnmiwin66
	com.hp.ov.nms.spi.traffic-master.Nnm.port	The HTTP Port that the NNMi management server uses	80
Secondary-NNM	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.username	The administrator username for NNMi	
	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.https.port	The HTTPS port used by the NNMi management server	
	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.hostname	The fully Qualified Domain Name (FQDN) for the NNMi management server	
	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.present	True if Secondary NNM has been configured and failover enabled	false
	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.port	The HTTP Port that the NNMi management server uses	
Primary-Shared-Drive	com.hp.ov.nms.spi.traffic-master.Nnm.perfspidatpath	The shared folder on NNMi management server that the Master collector and NPS use for storing the data collected by Master	/var/opt/OV/shared/perfSp
	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.perfspidatpath	The shared folder on NNMi management server that the Master collector and NPS use for storing the data collected by Master	
Secondary-Shared-Drive	com.hp.ov.nms.spi.traffic-master.nps.port	The port that the Master collector uses to connect to NPS Sybase database server	9303
	com.hp.ov.nms.spi.traffic-master.nps.sybase.user	The administrator username for NPS database	DBA
	com.hp.ov.nms.spi.traffic-master.nps.sybase.password	The administrator password for NPS database	*****

Updated: Monday, April 09, 2012 11:41:24 AM Total: 1

Once you click **Validate**, the right pane shows the success/failure messages as seen in the image below. The screen gives appropriate suggestions for failures.

	Title	Description	Value
Primary-NNM	com.hp.ov.nms.spi.traffic-master.Nnm.password	The administrator password for NNMi	traffic
	com.hp.ov.nms.spi.traffic-master.Nnm.username	The administrator username for NNMi	traffic
	com.hp.ov.nms.spi.traffic-master.Nnm.hostname	The fully Qualified Domain Name (FQDN) for the NNMi management server	nnmiwin66
	com.hp.ov.nms.spi.traffic-master.Nnm.port	The HTTP Port that the NNMi management server uses	80
	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.username	The administrator username for NNMi	
Secondary-NNM	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.https.port	The HTTPS port used by the NNMi management server	
	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.hostname	The fully Qualified Domain Name (FQDN) for the NNMi management server	
	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.present	True if Secondary NNM has been configured and failover enabled	false
	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.port	The HTTP Port that the NNMi management server uses	
	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.password	The administrator password for NNMi	
Primary-Shared-Drive	com.hp.ov.nms.spi.traffic-master.Nnm.perfspidatpath	The shared folder on NNMi management server that the Master collector and NPS use for storing the data collected by Master	/var/opt/OV/sha
	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.perfspidatpath	The shared folder on NNMi management server that the Master collector and NPS use for storing the data collected by Master	
Secondary-Shared-Drive	com.hp.ov.nms.spi.traffic-master.nps.port	The port that the Master collector uses to connect to NPS Sybase database server	9303
	com.hp.ov.nms.spi.traffic-master.nps.sybase.user	The administrator username for NPS database	DBA

When a failure is detected, error message appears in the following format:

The screenshot shows the 'Installation Verification' window in the Network Node Manager iSPI Performance for Traffic application. The left sidebar contains a tree view with categories like Configuration, System Health, Site, ToS and Threshold Configuration, Filter Configuration, Application Mapping Configuration, and Flow Forwarder and Flow Producer. The main area displays a table of verification steps. A red box highlights the 'NPS connection could not be established' error message next to the 'NPS Hostname' field.

Category	Step	Field	Description	Value
Primary-NM	Validation Success	NNM Password	The administrator password for NNM:	*****
		NNM Username	The administrator username for NNM:	traffic
		NNM Hostname	The fully Qualified Domain Name (FQDN) for the NNM management server	nnmha7
		NNM HTTP Port	The HTTP Port that the NNM management server uses	80
Secondary-NM	secondary nnm not configured	NNM SECONDARY Username	The administrator username for NNM:	
		NNM SECONDARY HTTPS Port	The HTTPS port used by the NNM management server	
		NNM SECONDARY Hostname	The fully Qualified Domain Name (FQDN) for the NNM management server	
		NNM SECONDARY Present	True if Secondary NNM has been configured and failover enabled	false
		NNM SECONDARY HTTP Port	The HTTP Port that the NNM management server uses	
Primary-Shared-Drive	Validation Success	NNM SPI Data Path	The shared folder on NNM management server that the Master collector and NPS use for storing the data collected by Master	/nnm_sharedN
		NNM SECONDARY SPI Data Path	The shared folder on NNM management server that the Master collector and NPS use for storing the data collected by Master	
NPS	secondary nnm not configured	NPS Port	The port that the Master collector uses to connect to NPS Sybase database server	9303
		NPS Sybase Username	The administrator username for NPS database	DBA
		NPS Sybase Password	The administrator password for NPS database	*****
		NPS Hostname	The fully Qualified Domain Name (FQDN) for the system where NPS and are installed	nnmep2

Updated: Monday, May 14, 2012 3:01:13 PM Total: 1

You can see the Traffic Health view to know more about the problem and suggested workarounds. Once the suggested changes are made, make sure the Master Collector process is re-started for the changes to take effect.

Note: For troubleshooting errors found in the verification stage, please refer to the NNM iSPI Performance for Traffic Deployment guide.

Configuring the Leaf Collector

For the NNM iSPI Performance for Traffic to start receiving flow packets from the routers and processing the records to show reports, it is mandatory to have the Leaf Collector configured first. It involved the following two tasks:

1. Configuring the Leaf Collector system – the system on which the Leaf Collector is installed
2. Configuring the logical Leaf Collectors for each Leaf Collector system

Configure the Leaf Collector System

After logging into the NNM iSPI Performance for Traffic Configuration form, click **Leaf Collector System**, and then click on the **New** button to add a Leaf Collector system.

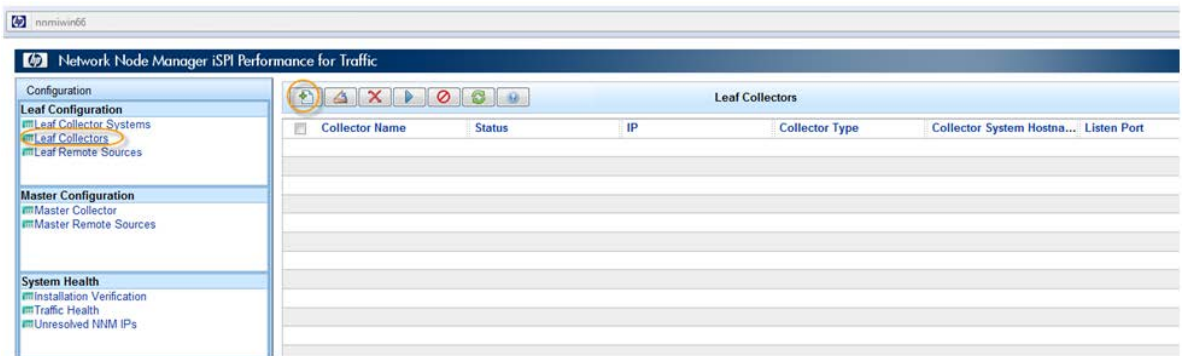
Once the Leaf Collector systems are configured, you must configure logical Leaf Collectors for each Leaf Collector system to start receiving flows from routers.

Best Practice: HP recommends that best performance of the SPI is seen when no more than 3 logical Leaf Collectors are configured for each Leaf Collector system.

It is mandatory to have one Leaf Collector configured for each flow type. That is, netflow, sflow, and IPFIX type of flow traffics should have one Leaf Collector configured each.

It is a good practice to forward the same type of flow traffic from multiple routers to the same port on the Leaf Collector system.

1. To configure the Leaf Collector, go to the NNM iSPI Performance for Traffic Configuration form, click **Leaf Collectors**, and then click **New**.



2. In the collector configuration form, type the following details:
 - Collector Name: A meaningful name to address this logical Leaf Collector
 - Collector Type: Select an appropriate value for a type of flow record
 - Listen Port: The port on which the router is exporting the flow records
 - IP: IP Address of the interface on which the Leaf Collector system receives flow records from the router. Use '0.0.0.0' if the routers send flow records to multiple interfaces on the Leaf Collector system (when the system is multi-homed).

Do not to set the "Store Flow in File" option to "true" unless there is a need to export the NNM iSPI Performance for Traffic-collected netflow data to third-party software for reporting and analysis purpose.

- Set the DNS Lookup of Source and Destination IPs as needed.
DNS lookup is done on the Leaf Collector system; therefore, it is required to have a well-performing DNS configuration on the Leaf Collector system.
3. Go to the "All Leaf Collector Systems" tab and select the system which you want the leaf collector to receive traffic data for.

Save & Close Save & New Help

Leaf Collector Details

Instructions

Configure the leaf collector to summarize the IP flow records.

Collector Name: NetFlowCollector

Collector Type: netflow

Listen Port: 9991

IP: 16.156.156.156

Store Flow in File: false

DNS

Source IP DNS Lookup: false

Destination IP DNS Lookup: true

All Filter Groups All Application Mapping Groups All TOS Groups All Leaf Collector Systems

Collector	System Hostname	HTTP Port	JNDI Port	Leaf Count
<input checked="" type="checkbox"/>	nmwini66	11080	11099	0

- Go the "All Application Mapping Groups" tab and make sure that the "DefaultAppMapGroup" is selected. Without this, application name will be seen as "Undefined" on reports.
- Click **Save & Close** to save this configuration.

Save & Close Save & New Help

Leaf Collector Details

Instructions

Configure the leaf collector to summarize the IP flow records.

Collector Name: NetFlowCollector

Collector Type: netflow

Listen Port: 9991

IP: 16.156.156.156

Store Flow in File: false

DNS

Source IP DNS Lookup: false

Destination IP DNS Lookup: true

All Filter Groups All Application Mapping Groups All TOS Groups All Leaf Collector Systems

Application Groups	Number of Application Mappings	Collector Name
<input checked="" type="checkbox"/> DefaultAppMapGroup	302	

- Once saved, make sure the Leaf Collector is seen in the "RUNNING" state. Wait for 2-3 minutes for the Leaf Collector to change the status to "RUNNING."

If the status does not get changed, click **Run** on the toolbar above (the  button)

Leaf Collectors					
<input type="checkbox"/>	Collector Name	Status	IP	Collector Type	Collector System Hostna... Listen Port
<input checked="" type="checkbox"/>	NetFlowCollector	RUNNING	16.156.156.156	netflow	nmwini66 and ip.com 9991

Note: When DNS Lookup is marked as "true" for Source or Destination, the time taken for the leaf to get into "RUNNING" state depends upon the DNS server performance. It is recommended that in such a case, you wait for 5-10 minutes before checking the Leaf collector status.

Validate Data Collection by the Leaf Collector

Once the Leaf collector is configured, verify that the Leaf Collector system is receiving and processing data from the router.

Click **NNM iSPI Performance for Traffic Leaf Collectors** from the Configuration workspace in the NNMi console and make sure the collectors are in the "RUNNING" state

Possible states are: RUNNING, NOTRUNNING, and STOPPEDBYUSER

The screenshot displays the HP Network Node Manager (NNM) interface. On the left, the 'Configuration' menu is expanded, showing various settings categories. The 'NNM ISPI Performance for Traffic Leaf Collectors' option is selected and highlighted with a red circle. The main panel shows the 'NNM ISPI Performance for Traffic Leaf Collectors' section. A table lists the collectors, with the 'Status' column for the 'NetFlowCollector' highlighted by a red circle and labeled 'RUNNING'. The bottom status bar indicates the data was updated on 4/9/12 at 12:04:37 PM, with a total of 1 object and 0 objects selected.

Collector Name	Status	Flow	Collector Ty	Container Hostname	IP	Listen Port
NetFlowCollector	RUNNING	✓	netflow	nnm-nf88 and hp.com	10.150.150.114	9991

Updated: 4/9/12 12:04:37 PM Total: 1 Selected: 0

Analysis

Summary

No Objects Selected

Double click a collector in the view to open the Leaf Collector form.

NNM iSPI Performance for Traffic Leaf Collectors Leaf Collector

General

Collector Name NetFlowCollector
 Status RUNNING
 Collector Type netflow
 IP 192.168.1.100
 Listen Port 9991
 Flow Processing Status Normal

Start-Stop Times

Last Start Time Mon, 9 Apr 2012 11:59:02
 Last Stop Time Never Stopped
 Last Flush Time Mon, 9 Apr 2012 12:12:28
 Number of Flows 224
 Number of Flushed 108
 Number of Packets 8

Collector System Details

Container Hostname nnm-nsd-1000-0000
 HTTP Port 11080
 JNDI Port 11099

Collector Statistics History

Last Flush Time	Number of Flows	Number of Flushed	Number of Packets
Mon, 9 Apr 2012 12:01:44	287	126	16
Mon, 9 Apr 2012 12:02:44	139	112	5
Mon, 9 Apr 2012 12:03:44	125	102	5
Mon, 9 Apr 2012 12:04:48	129	96	5
Mon, 9 Apr 2012 12:05:51	124	96	5
Mon, 9 Apr 2012 12:06:52	112	94	5
Mon, 9 Apr 2012 12:07:56	133	101	5
Mon, 9 Apr 2012 12:09:05	139	105	5
Mon, 9 Apr 2012 12:10:12	129	93	5
Mon, 9 Apr 2012 12:11:20	127	98	5
Mon, 9 Apr 2012 12:12:28	224	108	8

Review the following values to make sure the Leaf Collector is running correctly:

- “Last Flush Time” –the last time the Leaf Collector flushed the data to the Master Collector. Make sure this is close (1-2 mins) to the current system time
- “Collector Statistics History” - It shows the last 10-11 samples of data (1 min samples) with the Last Flush Time on each sample.
- “Flow Processing Status” – Shows the messages that indicate the health of the Leaf Collector
- In the NNM iSPI Performance for Traffic Configuration form, click **Flow Exporters** (under Flow Forwarder and Flow Producer) and make sure the routers configured to forward the data to Leaf Collector system are seen in this list.

Network Node Manager iSPI Performance for Traffic

Configuration

Leaf Configuration

- Leaf Collector Systems
- Leaf Collectors
- Leaf Remote Sources

Master Configuration

- Master Collector
- Master Remote Sources

System Health

- Installation Verification
- Traffic Health
- Unresolved NNM IPs

Site, ToS and Threshold Configuration

- Sites
- Type Of Service Groups
- Threshold

Filter Configuration

- Filters
- Filter Groups

Traffic Health

<input type="checkbox"/>	Collector	Severity	Start Time	End Time	Status	Message	Suggestion
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 00:26:24...	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 00:57:20...	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 01:27:37...	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 01:57:37...	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 02:27:45...	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 02:57:45...	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 03:28:09...	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 03:59:09...	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 04:30:04...	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 05:00:04...	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 05:32:56...	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 06:02:56...	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 06:37:55.51	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 07:07:57...	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 07:43:42.14	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 08:13:42...	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 08:50:26.60	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 09:20:26...	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 09:58:05...	-	INFO	Current size of the FL...	Removed 10K objects
<input type="checkbox"/>	NetFlowCollector	NORMAL	2012-04-13 10:28:06...	-	INFO	Current size of the FL...	Removed 10K objects

Open any message and see it in detail as follows:

Traffic Health

► Instructions

Problem Id 12
Collector NetFlowCollector
Severity NORMAL
Start Time 2012-04-13 00:57:20.184
End Time -
Message Current size of the FLOWRECORD object pool is 380000
Suggestion Removed 10K objects from the pool

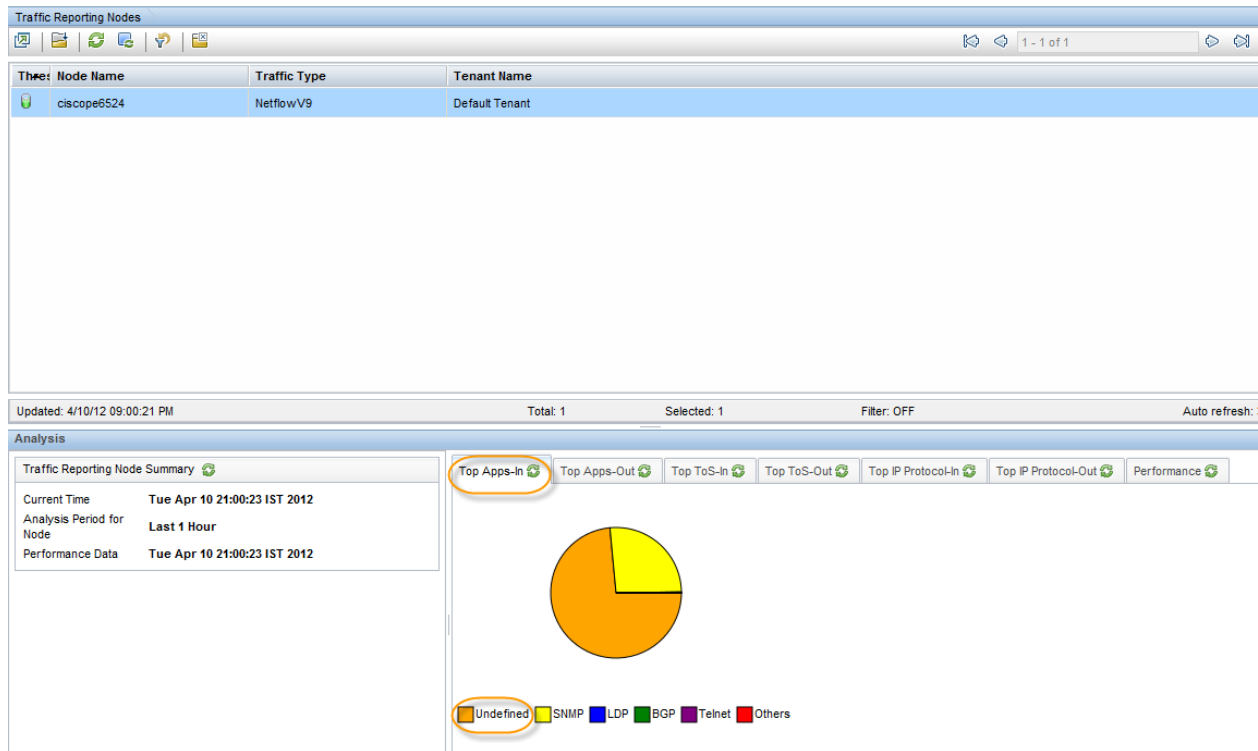
In the message, a Leaf Collector is represented by the name of the logical Leaf Collector and the Master Collector is represented by “Master.”

Configuring User-Defined Application Mapping

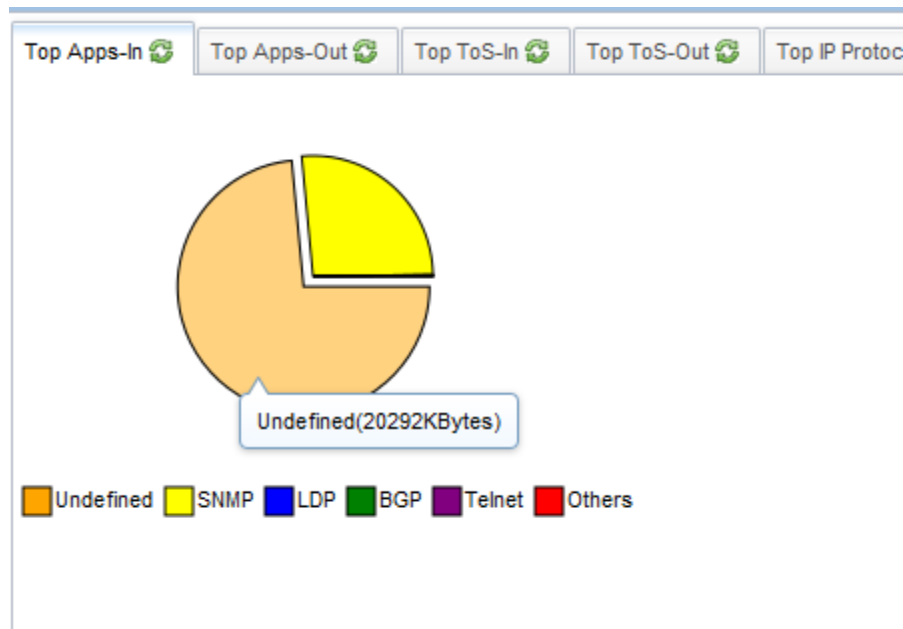
The NNM iSPI Performance for Traffic comes with 302 well-known mappings of ports and protocols to applications (like Port 22 for SSH, 23 for Telnet, and so on). However, if you want to have your own application mapping for applications running on non-standard ports, the iSPI provides you with a way to define a new application mapping.

1. First, go to the “Traffic Analysis” workspace in the NNMi console and go to the “Traffic Reporting Nodes” inventory view.

2. Select the router forwarding traffic and look at the “Top Apps-In” or “Top Apps-Out” tab to see the applications contributing to ingress or egress traffic flowing through this router. You will find some standard applications seen because of the Default Application mappings provided by the iSPI. You may also find an application with the name “Undefined,” which means there is no mapping defined for this traffic.



3. Mouse over on the pie that shows you the absolute Volume of the traffic (in KBs) that is 'Undefined.'



4. Go the “Undefined Applications” inventory in the Configuration UI of NNM iSPI Performance for Traffic.

5. You can see the port undefined traffic is destined to the router name and its interface from which traffic is being received along with the direction of the traffic (IN/OUT). Note down the port ranges for which there is a huge volume of traffic and for these port ranges, work with Network administrators to define this traffic.

Destination Port	Number of Bytes	Node Name	Interface Name	Ingress/Egress
2434	7000000	ciscope6524	Gi1/1	IN
17000	4613800	ciscope6524	Gi1/8	IN
18004	4600000	ciscope6524	Gi1/8	IN
2132	4600000	ciscope6524	Gi1/1	IN
64874	199836	ciscope6524	Gi1/1	IN
55052	199836	ciscope6524	Gi1/1	IN
60453	199436	ciscope6524	Gi1/1	IN
61556	199436	ciscope6524	Gi1/1	IN
771	103680	ciscope6524	Gi1/1	IN
0	84872	ciscope6524	Gi1/8	IN
0	76636	ciscope6524	Gi1/1	IN
2048	15384	ciscope6524	Gi1/1	IN
39823	15160	ciscope6524	Gi1/8	IN
3333	13800	ciscope6524	Gi1/1	IN
3432	13200	ciscope6524	Gi1/1	IN
1967	8160	ciscope6524	Gi1/1	IN
1967	7360	ciscope6524	Gi1/8	IN
38810	4415	ciscope6524	Gi1/1	IN
1281	3600	ciscope6524	Gi1/1	IN
39653	2548	ciscope6524	Gi1/8	IN
61985	2237	ciscope6524	Gi1/8	IN
56789	1408	ciscope6524	Gi1/1	IN
2816	1232	ciscope6524	Gi1/1	IN
148	768	ciscope6524	Gi1/8	IN
768	720	ciscope6524	Gi1/1	IN
62328	676	ciscope6524	Gi1/1	IN
64969	636	ciscope6524	Gi1/1	IN
55408	636	ciscope6524	Gi1/1	IN
51741	636	ciscope6524	Gi1/1	IN
				Total: 50

Updated: Tuesday, April 10, 2012 9:01:22 PM

To define traffic, you must define application mappings. These mappings can fall into one or more groups. All the mappings will always be part of "DefaultAppMapGroup".

Best Practice: HP recommends that you define a new Application Group first and then add the user-defined application mappings in that group. It is not recommended to change the Default group provided by the NNM iSPI Performance for Traffic.

6. Define a new application mapping group by launching the "Application Mapping Groups" configuration form:
 - a. Add a "New" group

Save & Close Save & New Help

Application Mapping Details

► Instructions

Application Name

▼ Application Mapping Details

Flow Attribute	Operation	Operand		
DstPort	>=	51,000	Add	Remove
ProducerIP				
SrcIP				
DstIP	<=	70,000	Add	Remove
IPProtocol				
NFSNMPInputIndex				
NFSNMPOutputIndex				
DstPort				
TCPFlags				
IPToS				

- e. Save and Close the application definition form and application mapping groups form.

Save & Close Save & New Help

Application Mapping Group Details

► Instructions

Application Groups

All Application Mappings

Application Name	Condition Configuration	Application Groups	Collector Name
DomainNameSystem	DstPort = 53	DefaultAppMapGroup	NetFlowCollector
DomainNameSystemRDNC...	DstPort = 953	DefaultAppMapGroup	NetFlowCollector
Doom	DstPort = 666	DefaultAppMapGroup	NetFlowCollector
EMCADS	DstPort = 3945	DefaultAppMapGroup	NetFlowCollector
EMWIN	DstPort = 2211	DefaultAppMapGroup	NetFlowCollector
EPP	DstPort = 700	DefaultAppMapGroup	NetFlowCollector
ERPApplication	DstPort >= 51000.DstPort <=...	DefaultAppMapGroup	NetFlowCollector
ESRO	DstPort = 259	DefaultAppMapGroup	NetFlowCollector
Echo	DstPort = 7	DefaultAppMapGroup	NetFlowCollector

Applying the configured application mappings

Once defined, the application mappings have to be applied to the Leaf Collectors.

1. Launch "Leaf Collectors" inventory view from the NNM iSPI Performance for Traffic configuration form.
2. Open the existing collector.

Network Node Manager iSPI Performance for Traffic

Leaf Configuration

Leaf Collector Systems

Leaf Collectors

Leaf Remote Sources

Master Configuration

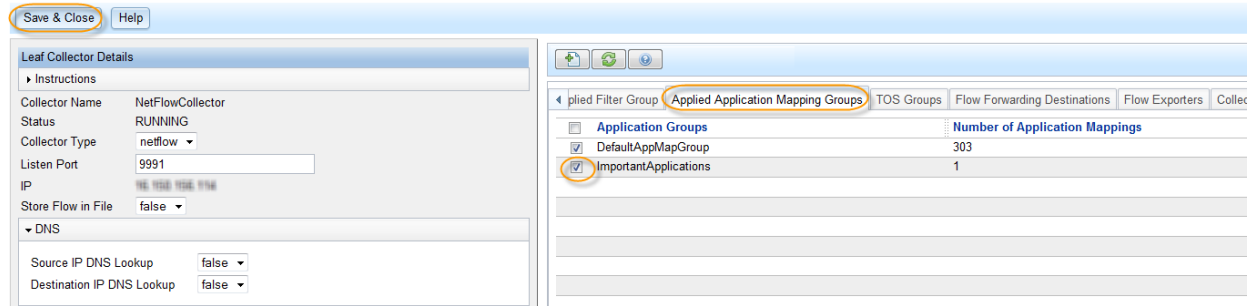
Master Collector

Master Remote Sources

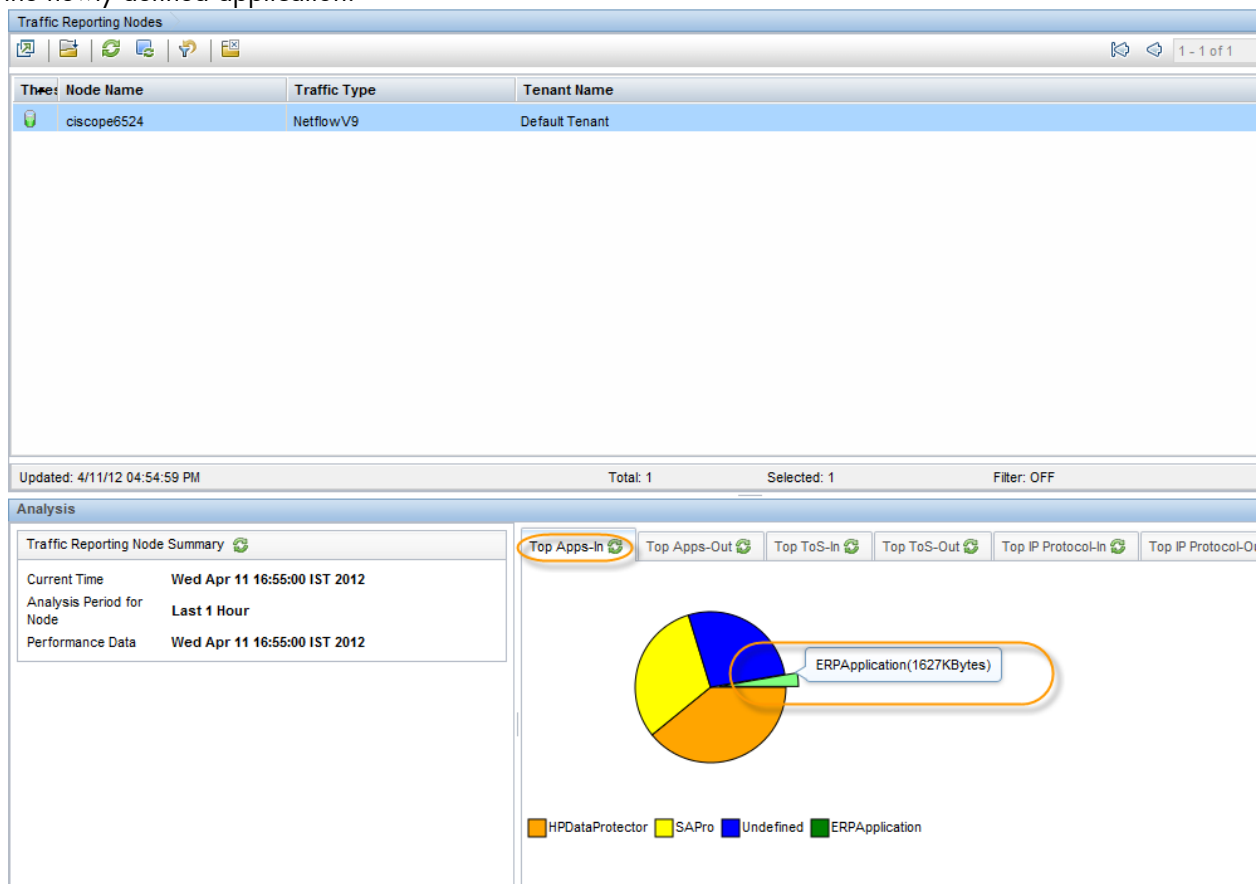
Leaf Collectors

Collector Name	Status	IP	Collector Type	Collector System Hostname...	Listen Port
NetFlowCollector	RUNNING	196.158.158.158	netflow	nmwin66.ind.hp.com	9991

3. Go to the “Applied Application Mappings Groups” tab and make sure the newly defined group ImportantApplications is checked.
4. Click “Save & Close.”



Wait for 15 mins and then look at the NNM iSPI Performance for Traffic node analysis pane to see the newly defined application.



Configuring ToS Groups

ToS (Type-of-Service) is the attribute in the traffic flow records that allow the user to find out the class/type of traffic. NNM iSPI Performance for Traffic allows the user to create a group for the combination of ToS values and name that traffic into a certain class like voice/video traffic. Unlike application mappings, NNM iSPI Performance for Traffic does not define any default ToS groups. To achieve this, follow these steps:

1. Click **Type Of Service Groups** in the NNM iSPI Performance for Traffic Configuration form and add a “New” configuration item.

Network Node Manager iSPI Performance for Traffic

Configuration

- Leaf Configuration
 - Leaf Collector Systems
 - Leaf Collectors
 - Leaf Remote Sources
- Master Configuration
 - Master Collector
 - Master Remote Sources
- System Health
 - Installation Verification
 - Traffic Health
 - Unresolved NNM IPs
- Site, ToS and Threshold Configuration
 - Sites
 - Type Of Service Groups**
 - Threshold

Type Of Service Groups

TOS Group Name	Number of TOS Mappings

2. Define the Group with a meaningful name for IPToS flow attribute. The operand value given for a condition here is what will appear on the reports and in the Traffic analysis panes.

Save & Close Save & New Help

Type Of Service Group Details

► Instructions

TOS Group Name VideoTraffic

▼ Type Of Service Group Details

Flow Attribute	Operation	TOS Number	Operand
IPToS	=	192	Video

Add Remove

Applying ToS Groups

Once defined, like Application mapping groups, ToS groups also have to be applied to the Leaf Collectors.

1. Launch the Leaf Collectors inventory from the Configuration form, open the Leaf collector detail form, and then go to “TOS Groups” tab and select the required groups.
2. “Save & Close” the configuration form, wait for 15 mins and find the ToS values on the reports.

Save & Close Help

Leaf Collector Details

Instructions

Collector Name: NetFlowCollector
 Status: RUNNING
 Collector Type: netflow
 Listen Port: 9991
 IP: 192.168.1.100
 Store Flow in File: false

DNS

Source IP DNS Lookup: false
 Destination IP DNS Lookup: true

Start-Stop Times

Last Start Time: Sat, 14 Apr 2012 19:54:20 IST
 Last Stop Time: Never Stopped
 Last Flush Time: Sun, 15 Apr 2012 11:53:43 IST
 Number of Flows: 136
 Number of Flushed: 92
 Number of Packets: 5

Applied Filter Group Applied Application Mapping Groups TOS Groups Flow Forwarding Destinations

TOS Group Name	Number of TOS Mappings
VoiceTraffic	1
VideoTraffic	1

Configuring Sites

Site in NNM iSPI Performance for Traffic is a simple way of grouping the Source and Destination IP Address ranges into a single logical entity. Based on which IP falls into the defined Site range, the sites are mapped as either Source site or Destination site for that traffic record.

1. Launch "Sites" inventory from the NNM iSPI Performance for Traffic configuration UI and add a "New" site.

hp Network Node Manager iSPI Performance for Traffic

Configuration

- Leaf Configuration
 - Leaf Collector Systems
 - Leaf Collectors
 - Leaf Remote Sources
- Master Configuration
 - Master Collector
 - Master Remote Sources
- System Health
 - Installation Verification
 - Traffic Health
 - Unresolved NNM IPs
- Sites, ToS and Threshold Configuration
 - Sites
 - Type Of Service Groups
 - Threshold

Sites

Site Name	Site Condition	Site Description	Site Priority	Tenant
Delhi	SrcIPLIKE[192.168.1.100] DstIPLIKE[192.168.1.100]		1	Default Tenant
Mumbai	SrcIPLIKE[192.168.1.100] DstIPLIKE[192.168.1.100]		20	Default Tenant
Bangalore	SrcIPLIKE[192.168.1.100] DstIPLIKE[192.168.1.100]		10	Default Tenant
Hyderabad	SrcIPLIKE[192.168.1.100] DstIPLIKE[192.168.1.100]		7	Default Tenant
FortCollins	SrcIPLIKE[192.168.1.100] DstIPLIKE[192.168.1.100]		9	Default Tenant

2. Provide the Site name, priority, and IP ranges in the definition. Priority is for the overlapping site ranges. The highest priority is indicated by 1. A higher number indicates a lower priority.

Save & Close Save & New Help

Site Details

Instructions

Site Name Enter the alphanumeric Site name(no spaces, no special characters except hyphen and underscore)

Tenant Default Tenant

Site Description

Site Priority

Site Priority

Show Higher Priority Sites Show Lower Priority Sites Show Same Priority Sites

Site IP Configuration

New IP/Range

All IP/Range

Add Remove Show Sites in the same IP Range

Once defined, Sites can be viewed in the Traffic analysis workspace by launching Sites inventory view.

Select a particular site and look at the analysis pane for Top Applications contributing to traffic for that site being a source or destination site.

HP Network Node Manager

User Name: system NNMI Role: Admin

File View Tools Actions Help

Incident Management Topology Maps Monitoring Troubleshooting Inventory Management Mode Incident Browsing Cisco IP Telephony Nortel IP Telephony Avaya IP Telephony Quality Assurance Traffic Analysis

Traffic Sites

Site Name	Site Priority	Site Description	Tenant Name
New York	10		Default Tenant
Boston	1		Default Tenant
Tokyo	9		Default Tenant
Shanghai	7		Default Tenant
Toronto	20		Default Tenant

Updated: 4/17/12 04:39:13 PM Total: 5 Selected: 1 Filter: OFF

Analysis

Site Summary

Current Time Tue Apr 17 16:39:21

Analysis Period for Site Last 1 Hour

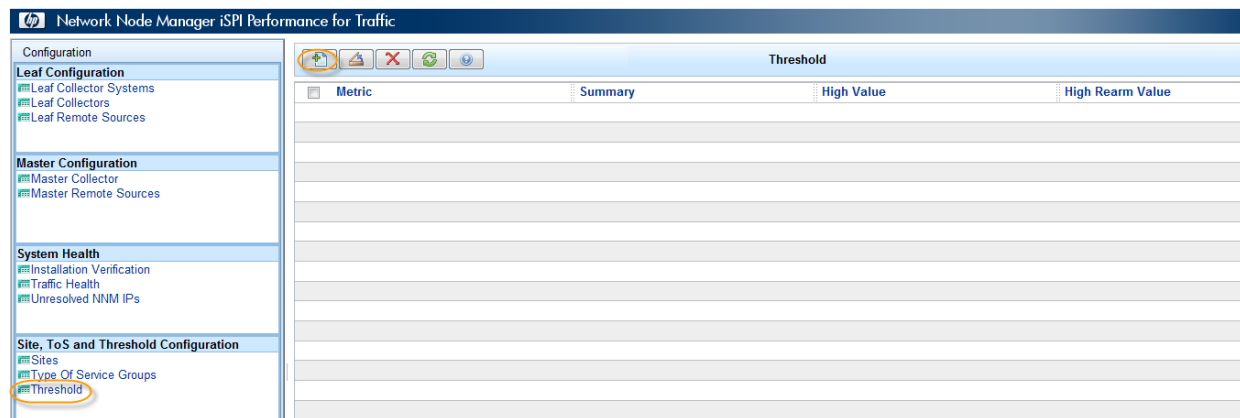
Source Site - Top Apps - In

HPDataProtector Undefined PriorityApp ERPApplication SAPro

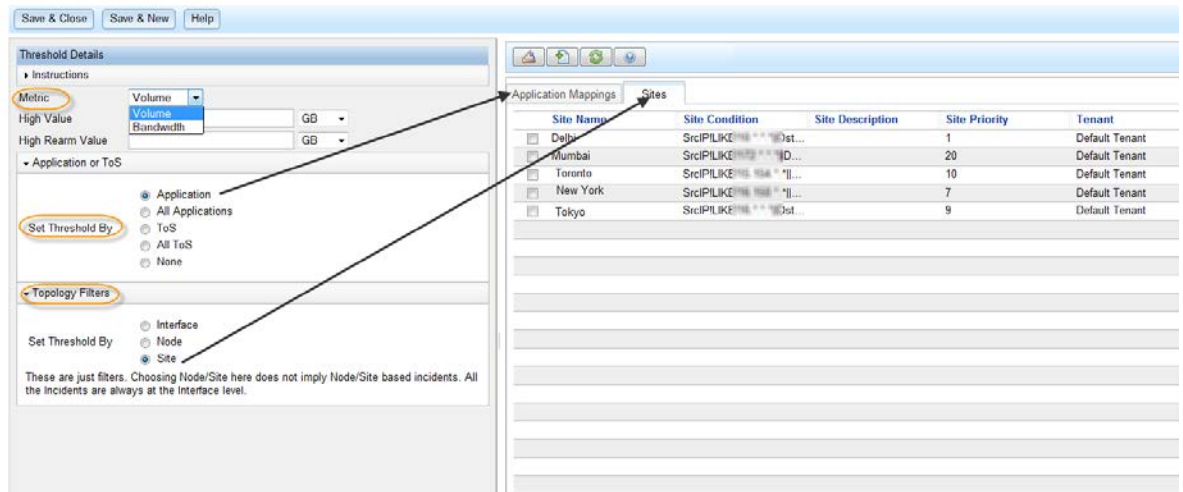
Configuring Thresholds

NNM iSPI Performance for Traffic also provides an option to configure threshold based on the volume or bandwidth of the traffic for the application(s) and ToS. Thresholds can be defined with the topology scope of Node, Interface, or Site.

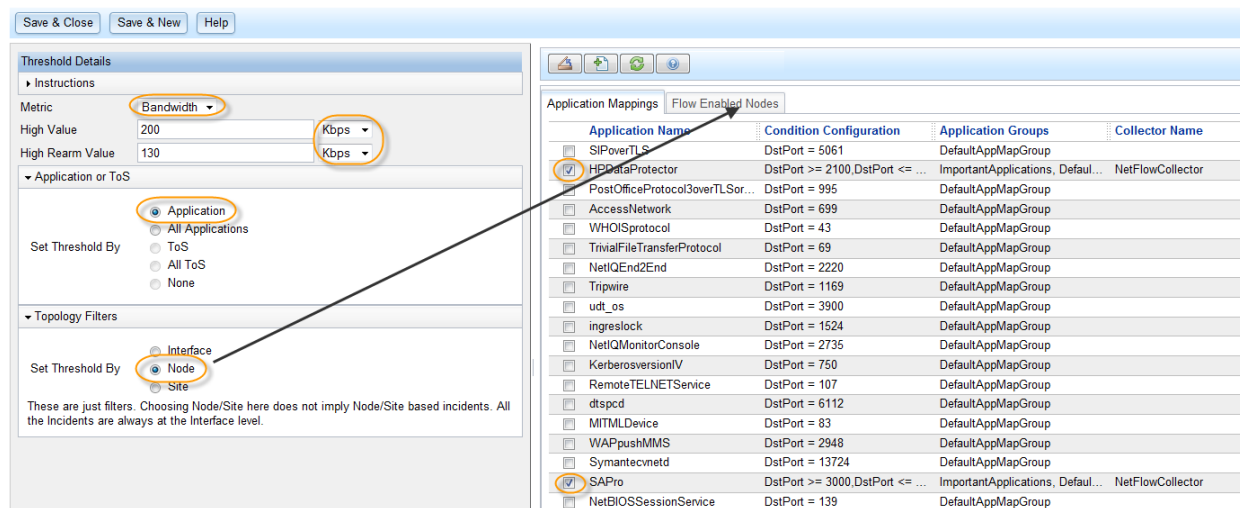
1. Click **Threshold** in the NNM iSPI Performance for Traffic Configuration form and add a “New” configuration item.



2. Select a Metric followed by the “Threshold By” option and then a Topology filter.



3. Based on these selections, you will see the tabs changing in the right pane.



Volumes are measure in Bytes while Bandwidth is measure in bps.

- For a selected topology filter, select the topology object (Site in the example below) you want to set the threshold on. No selection means all for the topology filter. For Application/ToS, either All or at least one needs to be selected.

Save & Close Save & New Help

Threshold Details

Instructions

Metric Volume 100 KB

High Value 100 KB

High Rearm Value 50 KB

Application or ToS

Set Threshold By

- Application
- All Applications
- ToS
- All ToS
- None

Topology Filters

Set Threshold By

- Interface
- Node
- Site

These are just filters. Choosing Node/Site here does not imply Node/Site based incidents. All the Incidents are always at the interface level.

Application Mappings

Application Name	Condition Configuration	Application Groups	Collector Name
DanwareNetOpRemoteControl	DstPort = 1970	DefaultAppMapGroup	
DanwareNetOpSchool	DstPort = 1971	DefaultAppMapGroup	
Discard	DstPort = 9	DefaultAppMapGroup	
DomainNameSystem	DstPort = 53	DefaultAppMapGroup	
DomainNameSystemRDNC...	DstPort = 953	DefaultAppMapGroup	
Doom	DstPort = 666	DefaultAppMapGroup	
EMCADS	DstPort = 3945	DefaultAppMapGroup	
EMWIN	DstPort = 2211	DefaultAppMapGroup	
EPP	DstPort = 700	DefaultAppMapGroup	
ERPApplication	DstPort >= 51000, DstPort <= ...	ImportantApplications, Default...	NetFlowCollector
ESRO	DstPort = 259	DefaultAppMapGroup	
Echo	DstPort = 7	DefaultAppMapGroup	
FCIP	DstPort = 3225	DefaultAppMapGroup	
FTPControl	DstPort = 21	DefaultAppMapGroup	
FTPControloverTLSoSSL	DstPort = 990	DefaultAppMapGroup	
FTPData	DstPort = 20	DefaultAppMapGroup	
FTPDataoverTLSoSSL	DstPort = 989	DefaultAppMapGroup	
FileMaker6andWebSharing	DstPort = 591	DefaultAppMapGroup	
Fingerprotocol	DstPort = 79	DefaultAppMapGroup	

Bandwidth thresholds are available only for Application. Once defined, the thresholds can be seen in the Threshold inventory.

Network Node Manager iSPI Performance for Traffic

Configuration

- Leaf Configuration
 - Leaf Collector Systems
 - Leaf Collectors
 - Leaf Remote Sources
- Master Configuration
 - Master Collector
 - Master Remote Sources
- System Health
 - Installation Verification
 - Traffic Health
 - Unresolved NNM IPs
- Site, ToS and Threshold Configuration
 - Sites
 - Type Of Service Groups
 - Threshold

Threshold

Metric	Summary	High Value	High Rearm Value
VOLUME	Sites: 1, Applications: 1	100.0 KB	50.0 KB
BANDWIDTH	Flow Node: 1, Applications: 2	200.0 Kbps	130.0 Kbps

You can also configure threshold by selecting a node from the inventory of Traffic reporting nodes and right clicking **Configure Traffic Threshold**.

Traffic Reporting Nodes

Node Name	Traffic Type	Tenant Name
cisco6524	Netflow/V9	Default Tenant

Context Menu:

- Select All
- Sort
- Filter
- Export To CSV
- Configure Traffic Threshold
- Traffic Maps
- Traffic Reports
- Quality Assurance
- HP NNM iSPI Performance

Once defined, the applicable thresholds can be looked in the “Traffic Reporting Node” detail form in the “Applicable threshold” tab.

Traffic Reporting Nodes Traffic Reporting Node

General

Node Name: ciscope6524

Traffic Type: NetflowV9

Tenant Name: Default Tenant

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

Value	Value Unit	Rearm Value	Rearm Unit	Metric
100.0	KB	50.0	KB	Volume
200.0	Kbps	130.0	Kbps	Bandwidth

Updated: 4/17/12 04:57:26 PM Total: 2 Selected: 0 Filter: OFF Auto refresh: 3 min

Threshold violations result in the alerts and these alerts appear in the “Incidents” tab of the Traffic reporting node.

Traffic Reporting Nodes Traffic Reporting Node

General

Node Name: ciscope6524

Traffic Type: NetflowV9

Tenant Name: Default Tenant

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

Severity	Life	Last Occurrence Time	Correlation Nature	Source Node	Message
Critical		4/17/12 4:57:43 PM		ciscope6524	One or more interfaces on node: ciscope6524.ind.hp.com has breached the traffic thresholds

Updated: 4/17/12 04:57:53 PM Total: 1 Selected: 1 Filter: OFF Auto refresh: OFF

Analysis

Incident Summary: NodeTraffic

Performance Data: Tue Apr 17 16:58:03 IST 2012

Message: One or more interfaces on node: ciscope6524 has breached the traffic thresholds

Severity: Critical

Priority: com.hp.nms.incident.priority.High

Lifecycle State: Registered

RCA Active: false

Source Object: ciscope6524 (Traffic Node Table Data)

Created/Opened: 4/17/12 04:57 PM (Open for 20.3 seconds)

Details

Custom Attributes: ciscope6524 MIB Values Source Node: ciscope6524

Category: Performance

Family: Traffic

Correlation Nature: Root Cause

Origin: INNMi

Last Occurrence Time: April 17, 2012 4:57:43 PM

Source Node: ciscope6524

Source Object: ciscope6524

Traffic threshold violations can be seen on the “Threshold state” column of the Traffic Reporting Nodes inventory.

Traffic Reporting Nodes

Threshold State	Node Name	Traffic Type	Tenant Name
	ciscope6524	NetflowV9	Default Tenant

There are specific inventories for “Threshold Exception Reporting Interfaces” and Nodes. One can look at these inventories for a direct list of threshold violated objects.

The screenshot shows the Network Node Manager (NNMi) interface. On the left, the 'Incident Management' menu is expanded, and 'Threshold Exceptions Reporting Interfaces' is selected. The main pane displays a table of threshold exceptions:

Interface Name	Hosted On	Traffic Type	Flow Process	Tenant Name
Gi1/1	ciscope6524	NetflowV9	✓	Default Tenant

Below the table, the 'Analysis' pane shows a 'Traffic Reporting Interface Summary' for the current time (Tue Apr 17 16:59:26) and analysis period (Last 1 Hour). A pie chart displays the distribution of traffic types, with a legend indicating: HPDataProtector (orange), Undefined (yellow), ERPAApplication (blue), PriorityApp (green), and SAPro (purple).

See the “Open Key Incidents” view in the NNMi console and look for the “Traffic” family. You can see all the threshold violated alerts; the analysis pane shows details of which interfaces and which application traffics violated thresholds.

The screenshot shows the Network Node Manager (NNMi) interface with the 'Open Key Incidents' view selected. The main pane displays a table of open key incidents:

Severity	Priority	Life	Last Occurrence	Assigned To	Source Node	Source Object	Category	Family	Origin	Correlation	Message	Notes
2	High	4/17/12 4:57:43 PM			ciscope6524	Gi1/1	Traffic	Performance	High traffic ingress volume reported through an interface Gi1/1 on the node ciscope6524			
2	High	4/17/12 4:57:43 PM			ciscope6524	Gi1/1	Traffic	Performance	High traffic ingress bandwidth reported through an interface Gi1/1 on the node ciscope6524			
2	High	4/17/12 4:57:43 PM			ciscope6524	ciscope6524	Traffic	Performance	One or more interfaces on node: ciscope6524 has breached the traffic thresholds			

Below the table, the 'Analysis' pane shows an 'Incident Summary' for the interface 'ApplicationTraffic'. The 'Performance Data' section indicates a high traffic ingress bandwidth reported through an interface Gi1/1 on the node ciscope6524. The 'Message' section provides details about the threshold violation, including the configured threshold (200.0 Kbps) and the measured value (1082.3548847266425 Kbps).

Common Use Cases

Identifying the source of high interface utilization

The NNM iSPI Performance for Metrics generates an alert for High Input/Output utilization of an interface and the NNM iSPI Performance for Traffic then helps identifying why the interface utilization is shown high.

The screenshot displays the Network Node Manager (NNM) interface. The top section shows a list of incidents under 'Open Key Incidents'. The selected incident is 'High input utilization on interface Gi1/1', which is highlighted with a red box. The incident details are shown in the bottom section, including the message: 'High traffic ingress volume reported through an interface Gi1/1 on the node ciscope6524 ind.hp.com in D'. The incident is categorized as 'Traffic' and 'Performance'. The 'Details' pane on the right shows the 'Performance' section, indicating the root cause is 'Traffic' and the root cause is 'NNM'. The 'Last Occurrence Time' is 'April 17, 2012 4:57:43 PM'.

Severity	Priority	Life	Last Occurrence-Ti	Assigned To	Source Node	Source Object	Category	Family	Origin	Corr	Message	Not			
5	2	4/17/12 5:05:24 PM	ciscope6524	Gi1/1	Traffic	High input utilization on interface Gi1/1	High traffic ingress volume reported through an interface Gi1/1 on the node ciscope6524 ind.hp.com in D	One or more interfaces on node: ciscope6524 ind.hp.com has breached the traffic thresholds	NNM health status is now at Warning	Interface Down	The target address 172.16.113.9 is down.	QA Probe ciscope2051 ind.hp.com_18 TCP Connect failed to run. Reason: Oper state is Not	QA Probe _udpecho failed to run. Reason: Oper state is NotConnected.	QA Probe _jcp failed to run. Reason: Oper state is NotConnected.	Interface Down

Updated: 4/17/12 05:06:31 PM Total: 42 Selected: 1 Filter: ON Auto refresh: 30 sec

Incident Summary: InterfaceApplicationSiteTraffic

Performance Data: Tue Apr 17 17:06:49 IST 2012

Message: High traffic ingress volume reported through an interface Gi1/1 on the node ciscope6524 ind.hp.com in D

Severity: 5

Priority: 2

Life: 4/17/12 5:05:24 PM

Assigned To: ciscope6524

Source Node: ciscope6524

Source Object: Gi1/1

Category: Traffic

Family: Performance

Origin: NNM

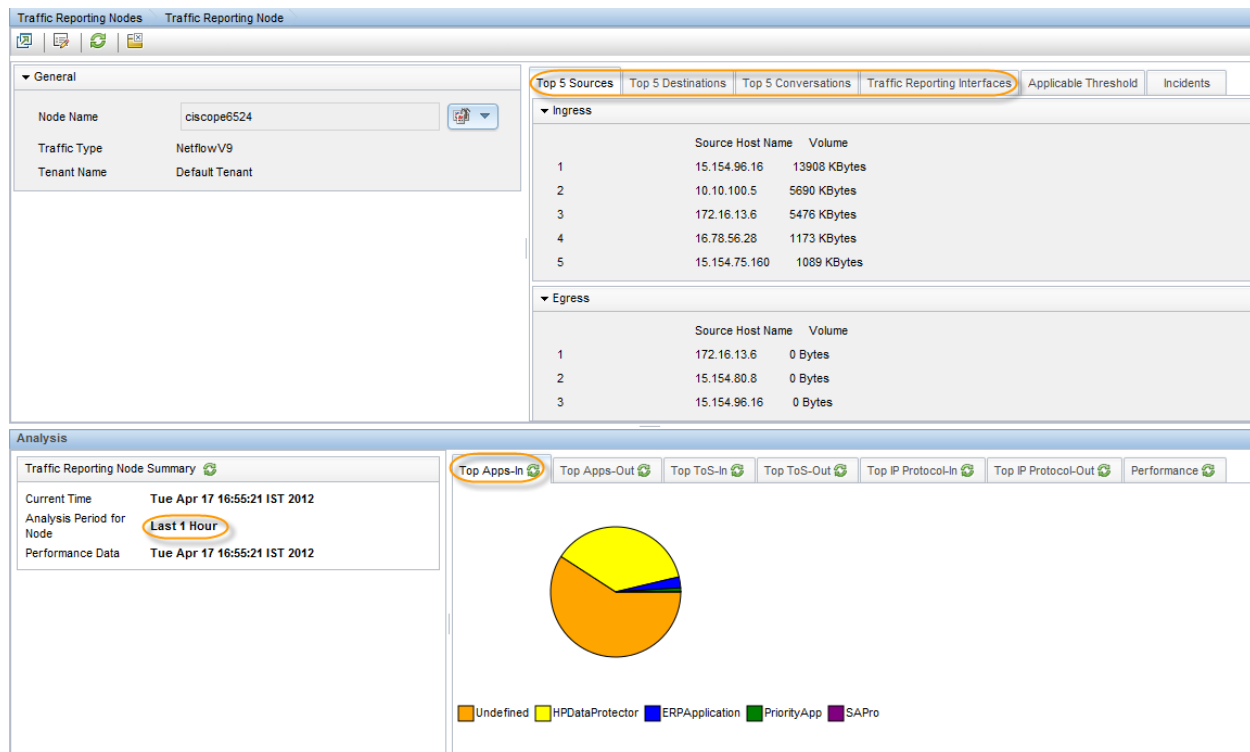
Correlation Nature: Root Cause

Last Occurrence Time: April 17, 2012 4:57:43 PM

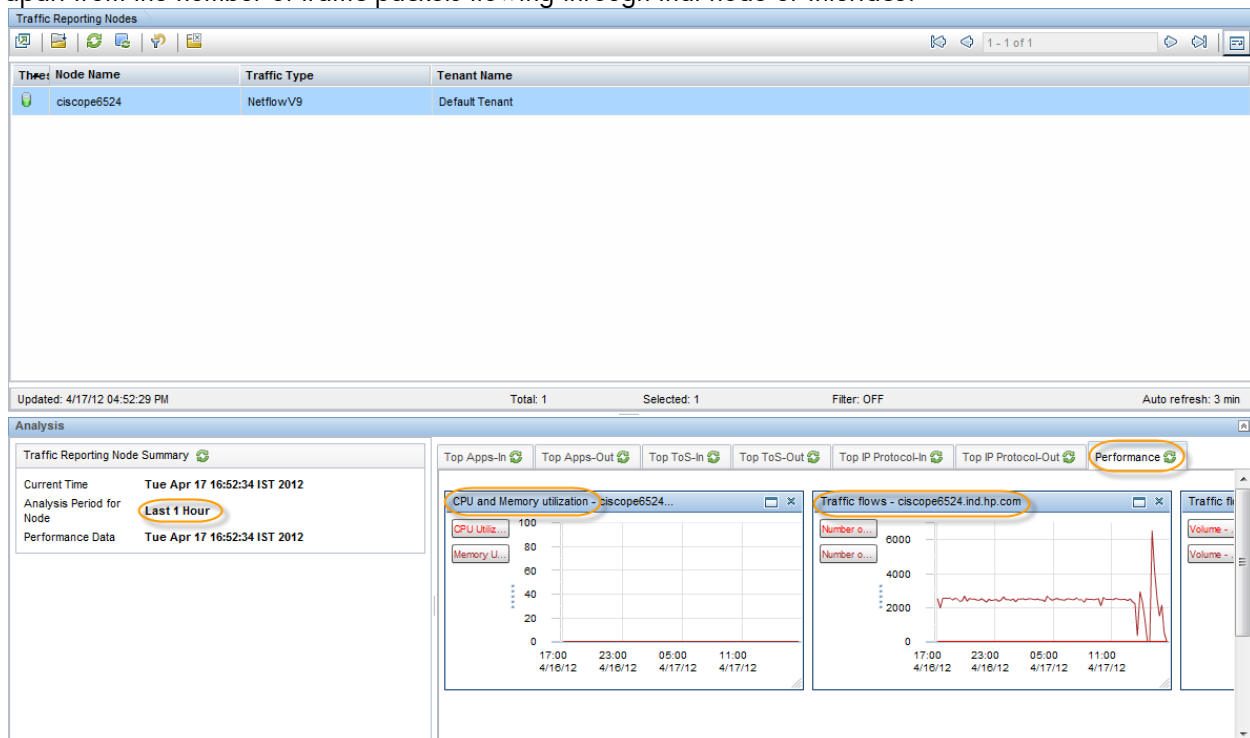
Source Node: ciscope6524

Source Object: Gi1/1

- Drilling down to the interface for which the management event is generated, you can look at the top 5 applications contributing to ingress/egress traffic through that interface
- You can also look at the Top Sources sending the traffic through that interface and also the top destinations to which the traffic is being forwarded as shown below in the image.
- As shown above, with thresholds configured in the NNM iSPI Performance for Traffic, you can also see NNM iSPI Performance for Traffic-specific threshold violation incidents getting generated and identify the exact application causing high utilization

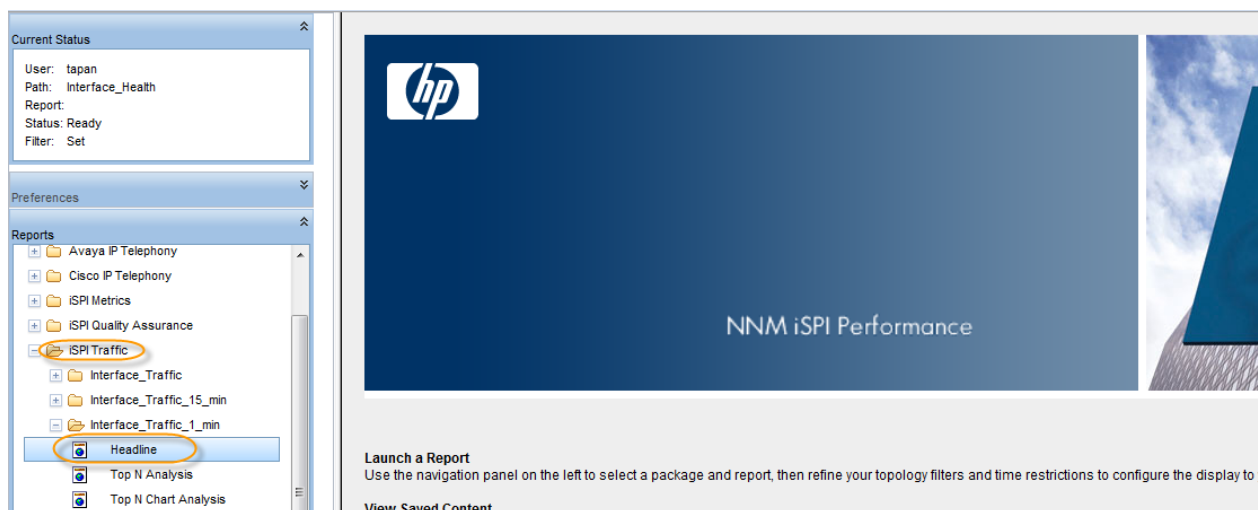


With the new "Performance" tab in the analysis pane, for a NNM iSPI Performance for Traffic node or interface, one can also look at the link utilization for an interface and CPU utilization for a node apart from the number of traffic packets flowing through that node or interface.

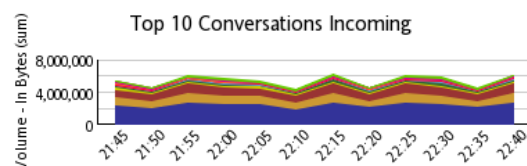


Viewing the summary of the network traffic distribution

With 9.20, the NNM iSPI Performance for Traffic introduces the “Headline” report. You can use this report to view the summary of the network traffic distribution. It provides Top contributors of traffic across the network.

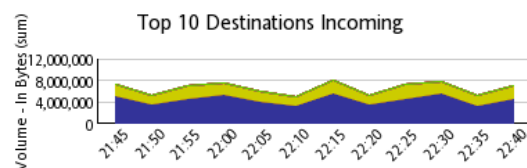


Apr 17, 2012 9:45:00 PM - Apr 17, 2012 10:45:00 PM (Last 1 Hour) (Server Time), Node Name = cscope6524



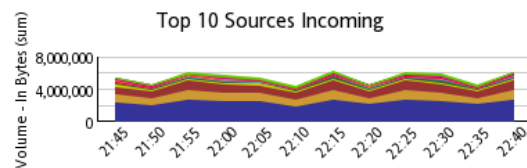
Source Host : Destination Host

175.154.94.116 : ... 10.10.100.5 : 10... 172.16.13.6 : 1... 116.78.116.200 : 1...



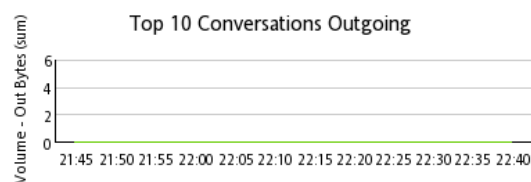
Destination Host Name

175.154.94.116 172.16.12.6 220.0.0.0 10.10.100.4 220.0.0.0



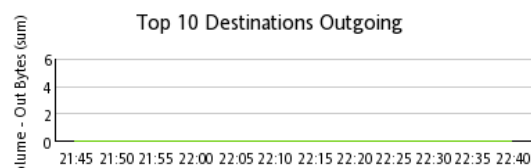
Source Host Name

175.154.94.116 10.10.100.5 172.16.13.6 116.78.116.200



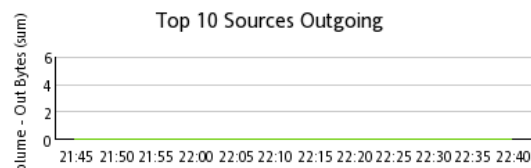
Source Host : Destination Host

10.10.100.3 : 10... 10.10.100.1 : 10... 10.10.100.2 : 10...



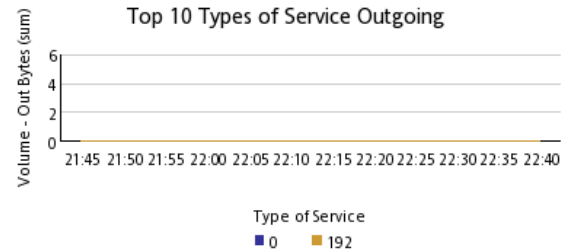
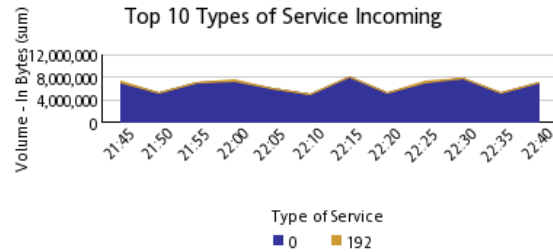
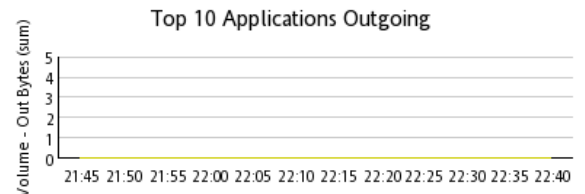
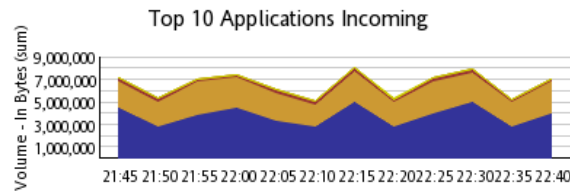
Destination Host Name

220.0.0.0 10.10.100.4 172.16.12.6 175.154.94.116 220.0.0.0



Source Host Name

10.10.100.3 10.10.100.1 10.10.100.2 10.10.100.5

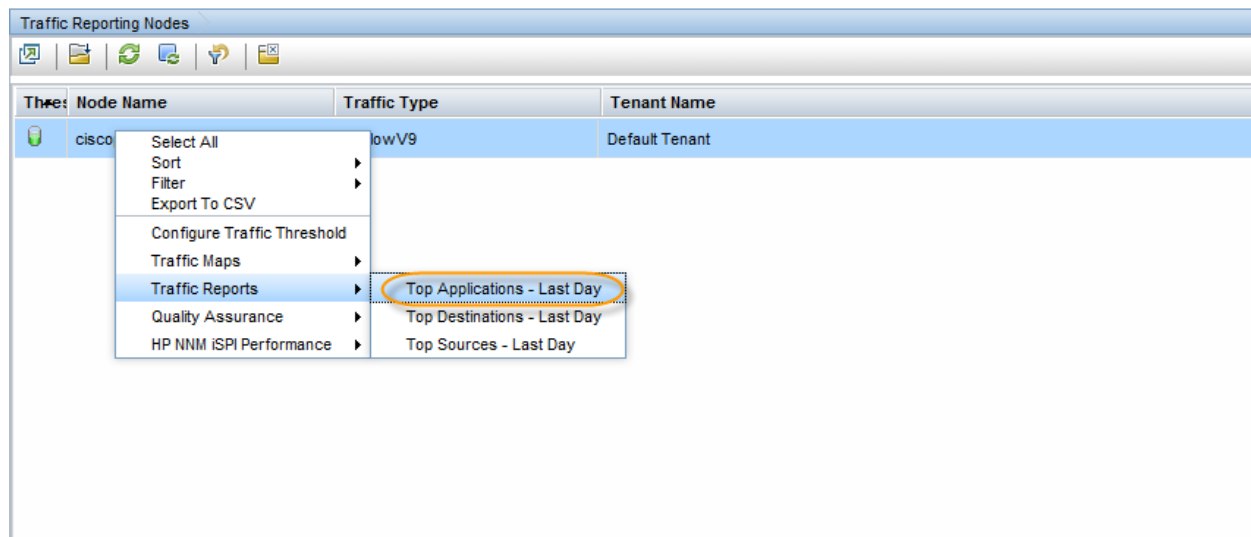


Generated at : 10:48:20 PM (Server Time)

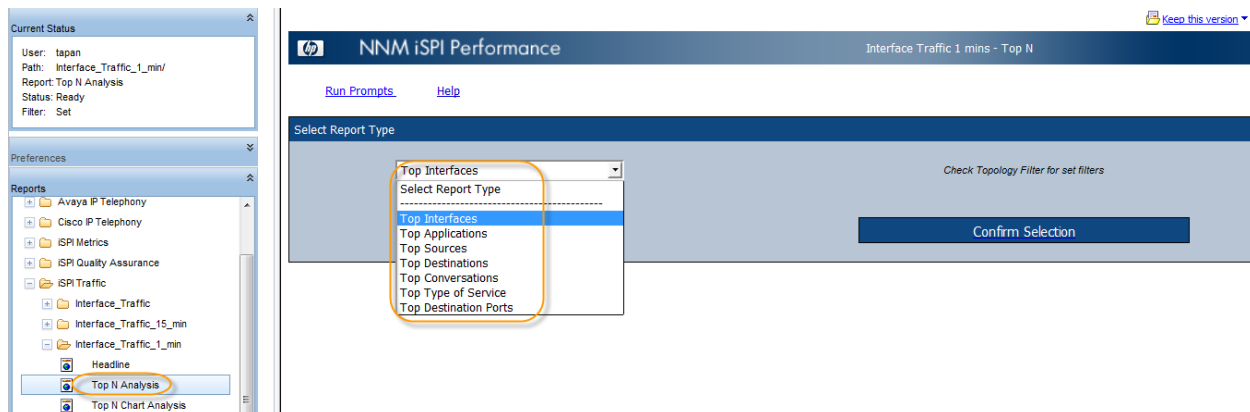
Interface_Traffic_1_min :: Headline - Mozilla Firefox

Analyze the network traffic trends

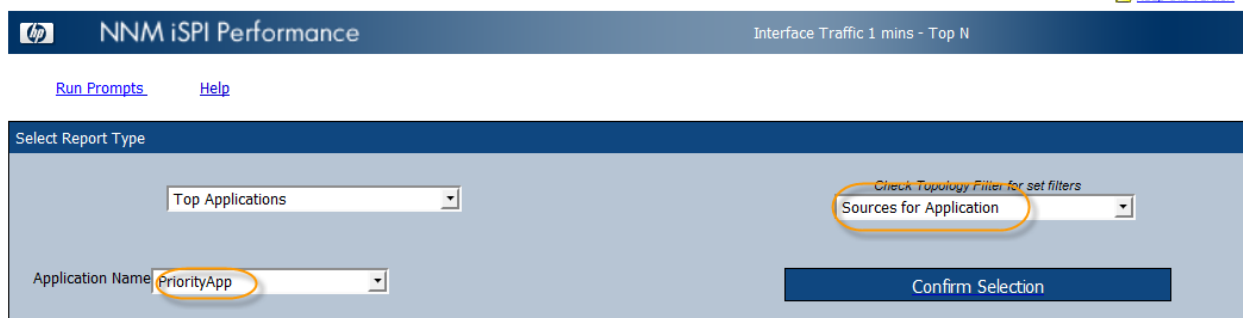
- You can analyze network traffic trends for daily, weekly and monthly aggregated data
- For daily, top applications traffic, right click a Traffic node and launch the "Top Applications – Last Day" report.
- It is a single click report that enables you to look at the Top Applications contributing traffic through that network device.



- You can directly launch the NNM iSPI Performance for Traffic reports from NPS report home page as well. At the top level, "Top N Analysis" link allows the user to quick launch different "Top Contributor" reports with a single click. For example, as shown below, select "Top Applications" as a report type



Drill down and select the application for which you want to see Top Sources
Select "Sources for Application" as the next level filter



"Confirm Selection" and one can see the report showing Top Sources for specific application(s).

Interface Traffic 1 min - Sources__For__Applications - Top N

Options Run Prompts Show Bookmark Help

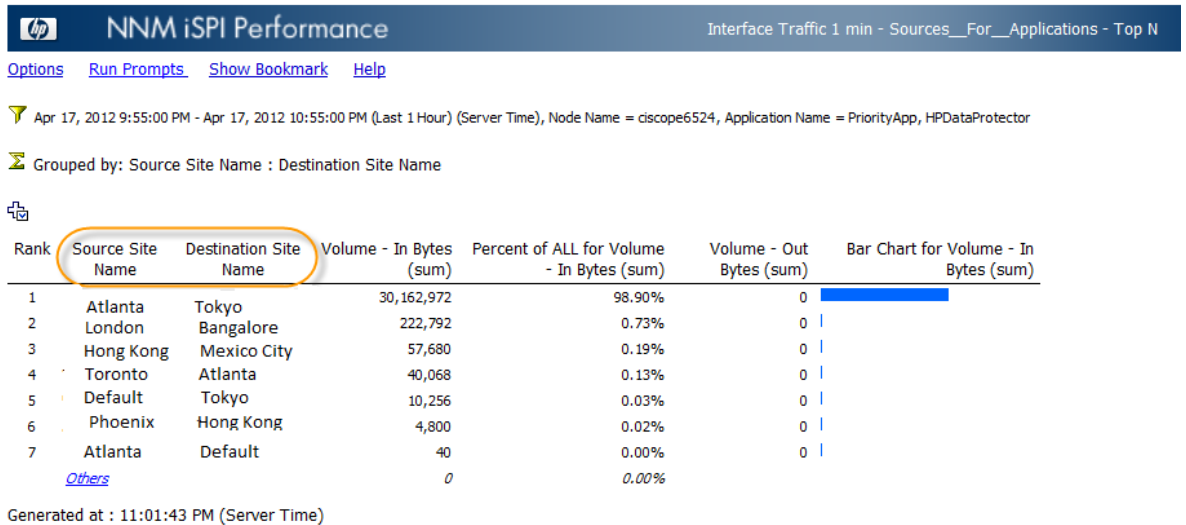
Apr 17, 2012 9:55:00 PM - Apr 17, 2012 10:55:00 PM (Last 1 Hour) (Server Time), Node Name = ciscope6524 Application Name = PriorityApp, HPDataProtector

Grouped by: Source Host Name

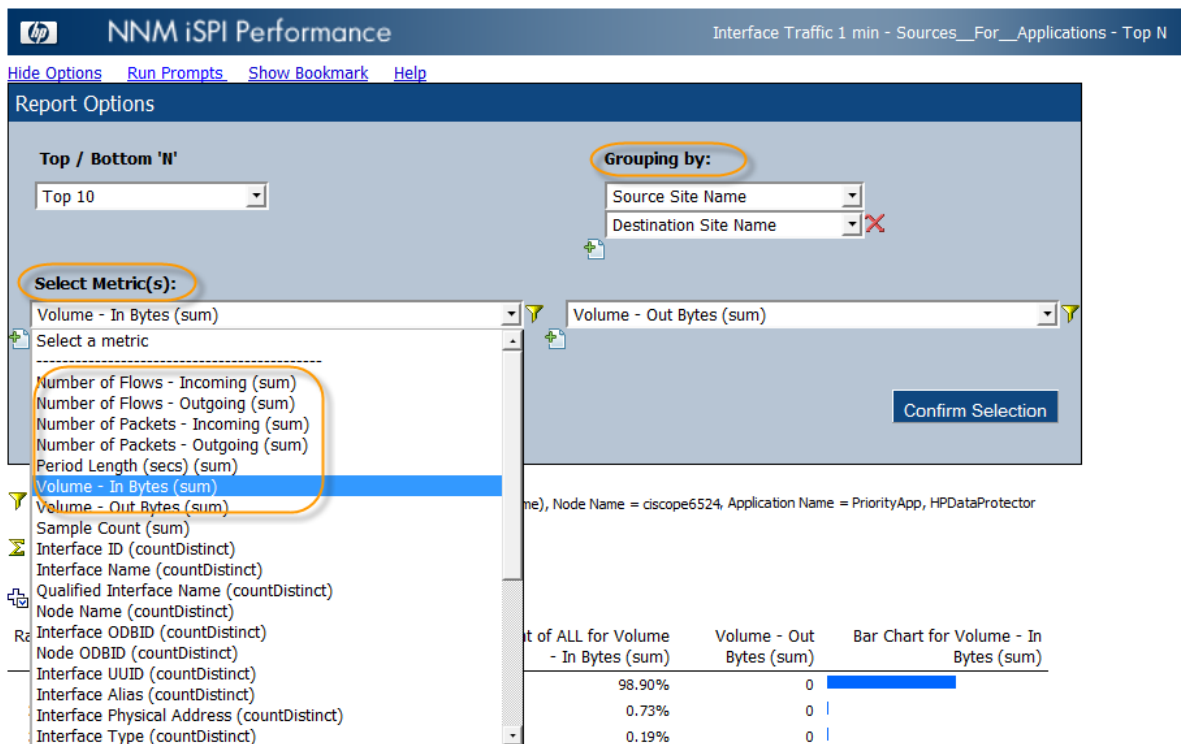
Rank	Source Host Name	Volume - In Bytes (sum)	Percent of ALL for Volume - In Bytes (sum)	Volume - Out Bytes (sum)	Bar Chart for Volume - In Bytes (sum)
1	10.10.10.10	30,127,760	98.78%	0	
2	10.10.10.10	211,872	0.69%	0	
3	10.10.10.10	57,680	0.19%	0	
4	10.10.10.10	25,668	0.08%	0	
5	10.10.10.10	14,400	0.05%	0	
6	10.10.10.10	9,680	0.03%	0	
7	10.10.10.10	5,124	0.02%	0	
8	10.10.10.10	5,040	0.02%	0	
9	10.10.10.10	4,800	0.02%	0	
10	10.10.10.10	4,800	0.02%	0	
	Others	31,784	0.10%		

Generated at : 10:59:30 PM (Server Time)

Similarly, you can also look at the traffic flowing from one site to the other site for a particular application – by selecting appropriate "Group By" options as shown below.

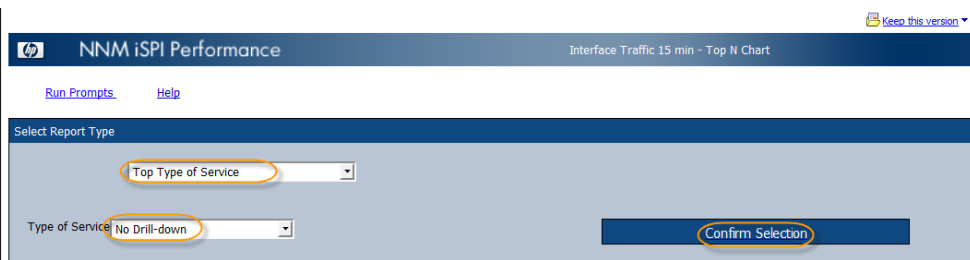
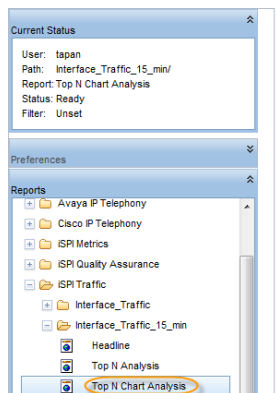


Following are the possible Metrics available to select from.

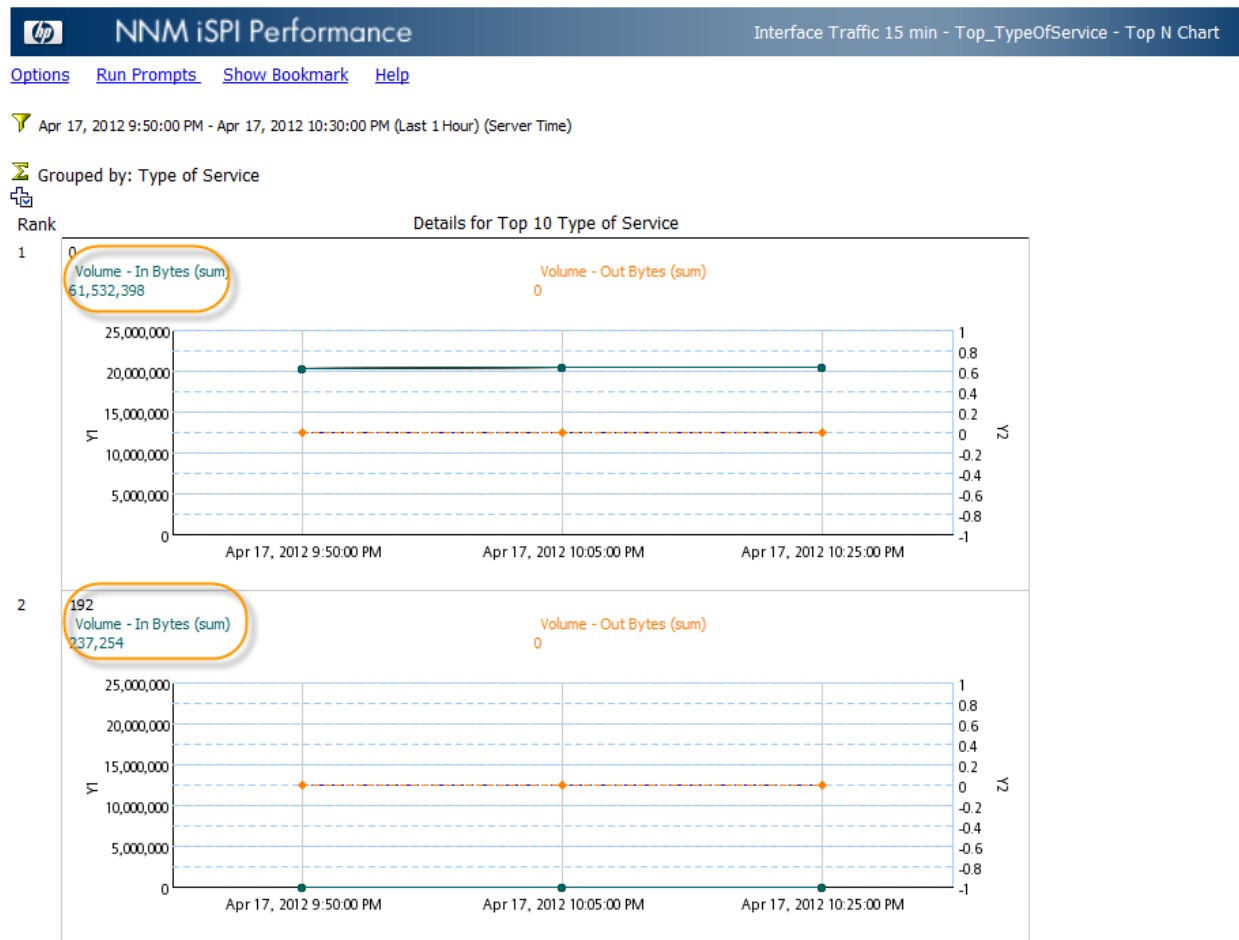


Similar to the applications, you can also look at the Class of traffic by using ToS and ToS groups related features of NNM iSPI Performance for Traffic:

1. Launch the 'Top ToS' report
2. Drill down and select "Top Sources for a ToS" and other such reports




3. Launch the report template needed.



Generated at : 11:04:49 PM (Server Time)

4. Select "Class of Service" as the Group by option to look at more meaningful name for a ToS value or the range or ToS values based on the ToS group configurations done in the SPI.

 **NNM iSPI Performance** Interface Traffic 15 min - Top_TypeOfService - Top N Chart

[Hide Options](#) [Run Prompts](#) [Show Bookmark](#) [Help](#)

Report Options

Top / Bottom 'N'

Top 10

Grouping by:

Class of Service

Select Metric(s):

Volume - In Bytes (sum)

Volume - Out Bytes (sum)

Confirm Selection

For more details about advanced concepts and workflows, refer to the *NNM iSPI Performance for Traffic Deployment Guide* and *Online Help*.

© 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. 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.

