HP Network Node Manager iSPI Performance for Traffic

Software Version: 9.20

Deployment by Example



Table of Contents

Introduction	
Assumptions	
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	
	10
Launching the NNM iSPI Pertormance for Trattic Contiguration Form	IC
Validating Installation	
Configuring the Leaf Collector	
Configure the Leaf Collector System	
Configure Collectors	
Validate Data Collection by the Leaf Collector	
Configuring User-Defined Application Mapping	
Configuring ToS Groups	
Configuring Sites	
Configuring Thresholds	
Common Use Cases	

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

HP NNMi Extension for iSPI Performance for Traffic 9.20.000	
HP Software Installer Plea	se Wait
MNMi Extension for iSPI Performance for Traffic	
NNMi User Name: System	
NNMi User Password: Retype Password:	
NNMI FQDN: nnmiwin66	
NNMi JNDI Port: 1099	ea
Traffic Master FQDN:	j leit.
Traffic Master http Port: 12080	
invent	
Cancel < Previous Ne:	kt >

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.

mary NNMI Server. Information	Required by Traffic ISPI	Secondary NNMI Server: Information	cion Requireu by Tranic ISPI
NNMI FQDN:	Innmiwin66	NNMI FQDN:	
NNMi HTTP Port:		NNMi HTTP Port	
NNMi HTTPS Port:		NNMI HTTPS Port:	
NNMi JNDI Port:		NNMi JNDI Port:	
Web Service Client User Name:		Web Service Client User Name:	
Web Service Client Password:		Web Service Client Password:	
Retype Password:		Retype Password:	
Perf SPI Data Path:		Perf SPI Data Path:	
(Is Secure? Is NNMi Failover Configured?		🗋 Is Secure?
affic iSPI Server: Information R	equired by NNMi		
Traffic FQDN:	nnmiwin66	Traffic User Name:	system
Traffic HTTP Port:		Traffic Password:	
Traffic HTTPS Port:		Retype Password:	
Traffic JNDI Port:		Ø	Is Secure?

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

😫 HP NNM iSPI Performa	ance for Traffi	c Master Collector 9.20.000		
HP S Performance	e SPI Server C	onfiguration		Please Wait
HP NNM iS	PI Performa	nce Server		
HostNam Port Num	iber: 🤇	9303		
HP NNM iS	PI Performa f the default	nce Database Configuration t UserName and Password	n has been modified.	ctor e a eft.
User nam	ie	DBA		
Password	1:	•••••		
Retype Pa	assword:	•••••		
		Ok		
Cancel			< Previous	Next >

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.

HP NNM iSPI Performance for T	raffic Leaf Collector 9.20.000	
HP Software Installer		Please Wait
Initialization Introduction		
🔬 Configuring Leaf		
Traffic Leaf FQDN:		
Traffic Leaf User Name: system		
Traffic Leaf Password:		
Retype Password:		
	Submit Clear	
42		
invent		
Cancel	< Pre	vious Next >

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

- 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 Collctor 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.

Configuration	Validate Li		Hadan Madification	
af Configuration	Validate	iip	niauon vernicauon	
Leaf Collector Systems		2.733	112007303010	1101150
Leaf Collectors		Title	Description	Value
Leaf Remote Sources		com.hp.ov.nms.spi.traffic-master.Nnm.https.port	The HTTPS port used by the NNMi management server	443
antes Conflorenting	-	com.hp.ov.nms.spi.traffic-master.Nnm.password	The administrator password for NNMi	traffic
aster Configuration				D Bring
Master Conector Master Remote Sources	Primary-NNM	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	nomiwin66.
stem Health		com.hp.ov.nms.spi.traffic-master.Nnm.port	The HTTP Port that the NNMi management server uses	80
Traffic Health Unresolved NNM IPs		com.hp.ov.nms.spi.traffic-master.Nnm.secondary.username	The administrator username for NNMi	
	6 .	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.https.port	The HTTPS port used by the NNMi management server	
ite, ToS and Threshold Configuration mSites mType Of Service Groups mThreshold		com.hp.ov.nms.spi.traffic-master.Nnm.secondary.hostname	The fully Qualified Domain Name (FQDN) for the NNMi management server	
	Secondary-NNM	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	
Iter Configuration				
Filters Filter Groups		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.perfspidatapath	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/perfS
oplication Mapping Configuration	Secondary- Shared-Drive	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.perfspidatapath	The shared folder on NNMi management server that the Master collector and NPS use for storing the data collected by Master	
Top N Application Inclusion List Undefined Applications		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
ow Forwarder and Flow Producer	NPS		The shall be a second for the second second	5161
Flow Exporters		com.np.ov.nms.spi.tramc-master.nps.sybase.password	The administrator password for NPS database	*****

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.

Validate H	elp	Installation Ve	rification	
				443
		com.hp.ov.nms.spi.traffic-master.Nnm.password	The administrator password for NNMi	traffic
Primary-NNM (Success	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	
		com.hp.ov.nms.spi.traffic-master.Nnm.secondary.https.port	The HTTPS port used by the NNMi management server	
seconda	secondary	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.hostname	The fully Qualified Domain Name (FQDN) for the NNMi management server	
Secondary-NNM	configured	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	Validation Success	com.hp.ov.nms.spi.traffic-master.Nnm.perfspidatapath	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
Secondary- Shared-Drive	secondary nnm not configured	com.hp.ov.nms.spi.traffic-master.Nnm.secondary.perfspidatapath	The shared folder on NNMi management server that the Master collector and NPS use for storing the data collected by Master	
		com.hp.ov.nms.spi.traffic-master.nps.port	The port that the Master collector uses to connect to NPS Sybase database server	9303
6	NPS	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:

Configuration	Validate	ala		Installation Verification		
Leaf Configuration	Tranciale I I	instance of the second				
mLeaf Collector Systems mLeaf Collectors mLeaf Remote Sources			NNM Password	The administrator password for NNMi		
	Primary-NNM	Validation Success	NNM Username	The administrator username for NNMi	traffic	
Master Configuration			NNM Hostname	The fully Qualified Domain Name (FQDN) for the NNMi management server	nnmiha7	
Master Remote Sources			NNM HTTP Port	The HTTP Port that the NNMi management server uses	80	
			NNM SECONDARY Username	The administrator username for NNMi		
System Health minstallation Venfication			NNM SECONDARY HTTPS Port	The HTTPS port used by the NNMi management server		
Trance NeedIn NIM IPs Site, ToS and Threshold Configuration Site Sites Type Of Service Groups Threshold	seconda Secondary-NNM nnm not configur	secondary	NNM SECONDARY Hostname	The fully Qualified Domain Name (FQDN) for the NNMi management server		
		M nnm not configured	NNM SECONDARY Present	True if Secondary NNM has been configured and failover enabled	false +	
			NNM SECONDARY HTTP Port	The HTTP Port that the NNMi management server uses		
			NNM SECONDARY Password	The administrator password for NNMi		
Filter Configuration	Primary- Shared-Drive	Validation Success	NNM SPI Data Path	The shared folder on NNNi management server that the Master collector and NPS use for storing the data collected by Master	/nnm_shared/	
minimer Groups	Secondary- Shared-Drive	secondary nnm not configured	NNM SECONDARY SPI Data Path	The shared folder on NNNi management server that the Master collector and NPS use for storing the data collected by Master		
Application Mapping Configuration	0		NPS Port	The port that the Master collector uses to connect to NPS Sybase database server	9303	
MApplication Mapping Groups Top N Application Inclusion List	NDC	NPS	NPS Sybase Username	The administrator username for NPS database	DBA	
MUndefined Applications	NP 5	be established	NPS Sybase Password	The administrator password for NPS database	•••••	
Flow Forwarder and Flow Producer		- stoonshold	NPS Hostname	The fully Qualified Domain Name (FQDN) for the system where NPS and are installed	nnmepr2	
eeriow Exporters	e		1	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.

NNM iSPI Performance for Traffic - Mozilla Firefox		
12080/nms-spi-traffic/	jsp	Ę
Metwork Node Manager iSPI Performation	mance for Traffic	
Configuration	A X C A Leaf Collector Systems	
Leaf Configuration	Lear conector systems	
Leaf Collector Systems	Collector System Hostname HTTP Port JNDI Port	
Eleaf Remote Sources		^
Master Configuration		
#Master Collector		
#Master Remote Sources		
Sustan Haalth		
Installation Verification		
Traffic Health		
III Unresolved NNM IP's		
=		
Site, ToS and Threshold Configuration		
Type Of Service Groups		
##Threshold		
Filter Configuration		
III Filters III Filter Groups IIII Filter		
Application Mapping Configuration		
Application Mappings		
Top N Application Inclusion List		
III Undefined Applications		
Flow Forwarder and Flow Producer	Updated: Wednesday, April 04, 2012 3:00:56 PM	Total: 1
112080/nms-spi-traffic/traffic	.jsp#	

Type the FQDN of the system on which the Leaf Collector is installed. Type the password that you chose during the installation of the Leaf Collector.

You must have one entry for each Leaf Collector system.

Save & Close Save & New	Help	
Collector System Details		
Instructions		
Collector System Hostname	mminimite and hp com-	
Leaf Password	•••••	
JNDI Port	11,099	
HTTP Port	11,080	

Configure Collectors

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**.

nomiwin66					
Ø Network Node Manager iS	Pl Performance for Traffic				
Configuration Leaf Configuration		0 3 9		Leaf Collectors	
Leaf Collector Systems Leaf Collectors Leaf Remote Sources	Collector Name	Status	IP	Collector Type	Collector System Hostna Listen Port
Master Configuration Master Collector Master Remote Sources					
System Health Installation Verification Intraffic Health INUnresolved NNM IPs					

- 2. In the collector configuration form, type the following details:
 - o Collector Name: A meaningful name to address this logical Leaf Collector
 - o Collector Type: Select an appropriate value for a type of flow record
 - o 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.

Leaf Collector Deta	ils		
- Instructions			
Configure the leaf	collector to summarize the IP flow records	All Filter Groups All Application Mapping Groups All TOS Groups All Leaf Collector Systems	
		Collector System Hostname HTTP Port JNDI Port	Leaf Count
Collector Name	NetFlowCollector	(I) nnmiwin66 11080 11099	0
Collector Type	netflow -	\checkmark	
Listen Port	9,991		
P	TRE TEED TEED THE		
Store Flow in File	false 👻		
- DNS			

- 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.
- 5. Click **Save & Close** to save this configuration.

Save & Close Sa	ve & New Help		
Leaf Collector Details			
Configure the leaf c	collector to summarize the IP flow records.	All Filter Groups All Application Mapping Groups	All TOS Groups All Leaf Collector Systems
Collector Name	NetFlowCollector	DefaultAppMapGroup	302
Collector Type	netflow 👻		
Listen Port	9,991		
IP	16. 158 158. 11a		
Store Flow in File	false 💌		
► DNS			
Source IP DNS Loo Destination IP DNS	kup false ▼ Lookup true ▼		
1. Onc	e saved, make sure the Leaf Collecto	r is seen in the "RUNNINC	9″ 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**)

	2 2 0	Lea	f Collectors		
Collector Name	Status	IP	Collector Type	Collector System Hostna	Listen Port
NetFlowCollector	RUNNING	16.150.156.114	netflow	mmiwin66 ind hp.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

Metwork Node Manager								
File View Tools Actions Help								
👌 Incident Management	*	NNM iSPI Performa	ince for Traffic Le	af Collec	tors			
🗛 Topology Maps	*	🗵 🖻 💋	😼 🖗 🗳					
Monitoring	≽	Collector Name	Status	Flow	Collector Tv	Container Hostname	IP	Listen Port
Troubleshooting	*	NetFlowCollector	RUNNING	0	netflow	minimized and he com	18.155.156.114	9991
1 Inventory	≽							
📀 Management Mode	≽							
🏠 Incident Browsing	≽							
👳 Traffic Analysis	≽							
4 Integration Module Configuration	岽							
🥕 Configuration	*							
 Communication Configuration Discovery Discovery Configuration Beeds 								
Tenants		Updated: 4/9/12 1	2:04:37 PM				Total: 1	Selected: 0
Overlapping Address Mappi		Analysis						
		Summary @						
		Summary 🦢						
			No Object	s Selec	ted			
+ Cuser Interface								
🖃 🧰 Security								
🛨 🧰 MIBs								
Device Profiles								
🗄 🧰 Object Groups								
RAMS Servers								
Management Stations (6.x/7.x)								
NNM iSPI Performance for Traffi								
NNM iSPI Performance for Traffi								

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

NNM iSPI Performance for T	raffic Leaf Collectors 🔷 Leaf Collector					
🖉 😼 😂 🖴						
✓ General		(Collector Statistics History Flow	v Processing Status		
Collector Name Status Collector Type	NetFlowCollector RUNNING netflow		▼ 図 ≧ ♡ ℝ ♥ Last Flush Time	Number of Flows	Number of Flushe	Number of Packets
Listen Port	9991		Mon, 9 Apr 2012 12:01:44	287	126	16
Flow Processing Status	Normal		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
Last Start Time	Mon, 9 Apr 2012 11:59:02		Mon, 9 Apr 2012 12:05:51	124	96	5
Last Stop Time	Never Stopped		Mon, 9 Apr 2012 12:06:52	112	94	5
Last Flush Time	Mon, 9 Apr 2012 12:12:28		Mon, 9 Apr 2012 12:07:56	133	101	5
Number of Flows	224		Mon, 9 Apr 2012 12:09:05	139	105	5
Number of Flushed	108		Mon, 9 Apr 2012 12:10:12	129	93	5
Number of Packets	8		Mon, 9 Apr 2012 12:11:20	127	98	5
- Collector System Details		11	Mon, 9 Apr 2012 12:12:28	224	108	8
Container Hostname HTTP Port JNDI Port	11080 11099					

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

- "Last Flush Rime" --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.

Metwork Node Manager iSPI Per	for	mance for Traffic			
Configuration		430	Flow Expor	ters	
Eeaf Collectors Eeaf Remote Sources		IP	Flow Node	Collector Name	Number of Flows
		112. 112.4: 102. 103	Giorgett24 and hp.com	NetFlowCollector	129
Master Configuration					
master Collector					
Im Master Remote Sources					
System Health					
Installation Verification					
Traffic Health					
Chresolved NNM IP's					
Site, ToS and Threshold Configuration					
# Sites					
	ш				
Filter Configuration					
Filters					
miller Groups					
Application Mapping Configuration					
Application Mappings					
Top N Application Inclusion List					
Imundefined Applications					
Flow Forwarder and Flow Producer					
Flow Forwarders		Updated: Monday, April 09	9, 2012 12:04:53 PM		Total: 1
	τ.				

If you see that the routers are exporting flow records but flows are not seen in the system configuration, click **Unresolved NNM IPs** in the NNM iSPI Performance for Traffic Configuration form.

If the IPs appear in this list, it means that the Master Collector is not able to get the topology object from NNMi for these IP addresses.

The reason could be these nodes are not discovered in NNMi as SNMP nodes or the Master Collector is not able to communicate with NNMi.

Metwork Node Manager iSPI Perfor	mance for Traffic			
Configuration		Unresolved NNM IF	Ps	
Leaf Configuration	IP	Interface Index	Last Attempt time	_
Master Configuration ■Master Collector ■Master Remote Sources				
System Health Important Station Verification Important Chealth Important Station St				
E Site, ToS and Threshold Configuration Sites Type Of Service Groups Threshold				
Filter Configuration I⊞Filters I≇Filter Groups				

To find out if Master and Leaf Collector health is fine, click **Traffic Health** in the NNM iSPI Performance for Traffic Configuration form.

Make sure no messages exist there (or at least there are no OPEN messages).

If an OPEN message exists, open the message and look at the detail for suggestions.

🕼 Network Node Manager iSPI Performance for Traffic							
Configuration East Collector Systems East Collectors Leaf Remote Sources	Collector Severity Start Time End Time Status Message Suggesti						
Master Configuration ﷺMaster Collector ﷺMaster Remote Sources							
System Health Imministallation Verification Imministraffic Health Immunresolved NNM IPs							

Some example traffic health messages are:

😥 Network Node Manager iSPI Performance for Traffic							
Configuration				Traffic Health			
mLeaf Collector Systems	Collector	Severity	Start Time	End Time	Status	Message	Suggestion
Eleaf Collectors	NetFlowCollector	NORMAL	2012-04-13 00:26:24	•	INFO	Current size of the FL	Removed 10K objects
and Lear Nemote Sources	NetFlowCollector	NORMAL	2012-04-13 00:57:20	-	INFO	Current size of the FL	Removed 10K objects
	NetFlowCollector	NORMAL	2012-04-13 01:27:37	-	INFO	Current size of the FL	Removed 10K objects
Master Configuration	NetFlowCollector	NORMAL	2012-04-13 01:57:37	-	INFO	Current size of the FL	Removed 10K objects
mMaster Collector mMaster Remote Sources	NetFlowCollector	NORMAL	2012-04-13 02:27:45	-	INFO	Current size of the FL	Removed 10K objects
	NetFlowCollector	NORMAL	2012-04-13 02:57:45	-	INFO	Current size of the FL	Removed 10K objects
	NetFlowCollector	NORMAL	2012-04-13 03:28:09	-	INFO	Current size of the FL	Removed 10K objects
System Health	NetFlowCollector	NORMAL	2012-04-13 03:59:09	-	INFO	Current size of the FL	Removed 10K objects
Installation Verification	NetFlowCollector	NORMAL	2012-04-13 04:30:04	-	INFO	Current size of the FL	Removed 10K objects
Traffic Health	NetFlowCollector	NORMAL	2012-04-13 05:00:04		INFO	Current size of the FL	Removed 10K objects
	NetFlowCollector	NORMAL	2012-04-13 05:32:56	-	INFO	Current size of the FL	Removed 10K objects
	NetFlowCollector	NORMAL	2012-04-13 06:02:56	-	INFO	Current size of the FL	Removed 10K objects
Site, ToS and Threshold Configuration	NetFlowCollector	NORMAL	2012-04-13 06:37:55.51	-	INFO	Current size of the FL	Removed 10K objects
Type Of Service Groups	NetFlowCollector	NORMAL	2012-04-13 07:07:57	-	INFO	Current size of the FL	Removed 10K objects
mThreshold	NetFlowCollector	NORMAL	2012-04-13 07:43:42.14	-	INFO	Current size of the FL	Removed 10K objects
	NetFlowCollector	NORMAL	2012-04-13 08:13:42	-	INFO	Current size of the FL	Removed 10K objects
Filter Configuration	NetFlowCollector	NORMAL	2012-04-13 08:50:26.60	÷	INFO	Current size of the FL	Removed 10K objects
#Filters	NetFlowCollector	NORMAL	2012-04-13 09:20:26	-	INFO	Current size of the FL	Removed 10K objects
##Filter Groups	NetFlowCollector	NORMAL	2012-04-13 09:58:05	-	INFO	Current size of the FL	Removed 10K objects
	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 Collector Severity Start Time End Time Message Suggestion	12 NetFlowCollector NORMAL 2012-04-13 00:57:20.184 - Current size of the FLOWRECORD object pool is 380000 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.

Traffic Reporting Nodes								
🖉 🗃 🥔 🗟 🎺 🗉	×				Ø	1 - 1 of 1	0 (\geqslant
Thee: Node Name	Traffic Type	Tenant Name						
ciscope6524	NetflowV9	Default Tenant						
Updated: 4/10/12 09:00:21 PM Analysis		Total: 1	Selected: 1		Filter: OFF		Auto refre	ish: (
Traffic Reporting Node Summary	G	Top Apps-In 🕄 Top Apps-Out 🕄	Top ToS-In 🔀	Top ToS-Out 💕	Top IP Protocol-In 🜮	Top IP Protocol-Out 🥵	Performance 🙄	
Current Time Tue Apr Analysis Period for Node Last 1 Ho Performance Data Tue Apr	10 21:00:23 IST 2012 our 10 21:00:23 IST 2012		BGP Teinet	Others				

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.

Configuration			Undefined Application	15	
eaf Configuration			ana		
Leaf Collector Systems	Destination Port	Number of Bytes	Node Name	Interface Name	Ingress/Egress
Leaf Remote Sources	2434	7000000	ciscope6524	Gi1/1	IN
	17000	4613800	ciscope6524	Gi1/8	IN
	18004	4600000	ciscope6524	Gi1/8	IN
aster Configuration	2132	4600000	ciscope6524	Gi1/1	IN
Master Remote Sources	64874	199836	ciscope6524	Gi1/1	IN
	55052	199836	ciscope6524	Gi1/1	IN
	60453	199436	ciscope6524	Gi1/1	IN
vstem Health	61556	199436	ciscope6524	Gi1/1	IN
Installation Verification	771	103680	ciscope6524	Gi1/1	IN
Traffic Health	0	84872	ciscope6524	Gi1/8	IN
Onresolved NNM IP's	0	76636	ciscope6524	Gi1/1	IN
	2048	15384	ciscope6524	Gi1/1	IN
te, ToS and Threshold Configuration	39823	15160	ciscope6524	Gi1/8	IN
Sites Type Of Service Groups	3333	13800	ciscope6524	Gi1/1	IN
Threshold	3432	13200	ciscope6524	Gi1/1	IN
	1967	8160	ciscope6524	Gi1/1	IN
Iter Configuration	1967	7360	ciscope6524	Gi1/8	IN
Filters	38810	4415	ciscope6524	Gi1/1	IN
Filter Groups	1281	3600	ciscope6524	Gi1/1	IN
	39653	2548	ciscope6524	Gi1/8	IN
	61985	2237	ciscope6524	Gi1/8	IN
oplication Mapping Configuration	56789	1408	ciscope6524	Gi1/1	IN
Application Mappings	2816	1232	ciscope6524	Gi1/1	IN
Top N Application Inclusion List	148	768	ciscope6524	Gi1/8	IN
Undefined Applications	768	720	ciscope6524	Gi1/1	IN
	62328	676	ciscope6524	Gi1/1	IN
Forwarder and Flow Producer	64969	636	ciscope6524	Gi1/1	IN
Flow Exporters	55408	636	ciscope6524	Gi1/1	IN
And a second	51754	252		Gi1/1	IN

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 userdefined 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

Metwork Node Manager iSPI Perfa	ormance for Traffic		
Out formation			
Configuration		Application Mapping Groups	
Leaf Collector Systems MLeaf Collectors	Application Groups	Number of Application Mappings	Collector Name
■Leaf Remote Sources	DefaultAppMapGroup	302	NetFlowCollector
Master Configuration			
mMaster Collector Master Remote Sources			
System Health			
Installation Verification			
In Tranc Health			
Site ToS and Threshold Configuration			
mSites			
Type Of Service Groups			
in callud			
Filter Configuration			
#Filters			
#Filter Groups			
Application Mapping Configuration			
Application Mappings			
Top N Application Inclusion List			
michidelined Applications			

b. Name it, for example, "Important Applications." For this new group, either chose the applications from within the default group or add a "New" application.

Save & Close Save & New Help				
Application Mapping Group Details				
Application Groups (ImportantApplications)	All Application Mappings			
	Application Name Condition Configura	ation Application Groups Collector Name	е	
	Telnet DstPort = 23	DefaultAppMapGroup NetFlowCollecto	or	
	gnutellasvc DstPort = 6346	DefaultAppMapGroup NetFlowCollecto	or	
	MicrosoftDSActiveDirectory DstPort = 445	DefaultAppMapGroup NetFlowCollecto	or	
	MATIPTypeA DstPort = 350	DefaultAppMapGroup NetFlowCollecto	or	
	IBMLotusNotesRPC DstPort = 1352	DefaultAppMapGroup NetFlowCollecto	or	
	DstPort = 750	DefaultAppMapGroup NetFlowCollecto	or	
	FileMaker6andWebSharing DstPort = 591	DefaultAppMapGroup NetFlowCollecto	or	

- c. In the "New" application mapping form, provide the application name. This is the name that will be visible in the Pie Chart of analysis pane and on the reports.
- d. In the details section, define the conditions for this application by selecting an appropriate "Flow Attribute" and "Operation."

Save & Close Save & New Help	
Application Mapping Details	
Instructions	
Application Name ERPApplication	Application Mapping Text Configuration All Application Mapping Groups
✓ Application Mapping Details	DstPort >= 51000, DstPort <= 70000, App = ERPApplication
Flow Attribute Operation Operand	
DstPort >= 51,000 Add Remove	
DstPort • <= • 70000 Add Remove	

Possible Flow attributes can be seen in the image below:

Save & Close Save & New Help				
Application Mapping [Details			
 Instructions 				
Application Name	ERPA	Application		
- Application Mappin	g Deta	ils		
Flow Attribut	e	Operation	Operand	
DstPort	-	>= 💌	51,000	Add Remove
ProducerIP SrcIP DstIP IPProtocol NFSNMPInputInde NFSNMPOutputInd DstPort TCPFlags IPToS	x lex	<= ▼	70,000	Add Remove

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

Save & Close Save & New Help					
Application Mapping Group Details					
Application Groups ImportantApplications	All Application Mappings				
	Application Name Condition Configuration Ap	plication Groups Collector Name			
	DomainNameSystem DstPort = 53 Def	faultAppMapGroup NetFlowCollector			
	DomainNameSystemRDNCS DstPort = 953 Def	faultAppMapGroup NetFlowCollector			
	Doom DstPort = 666 Def	faultAppMapGroup NetFlowCollector			
	EMCADS DstPort = 3945 Def	faultAppMapGroup NetFlowCollector			
	EMWIN DstPort = 2211 Def	faultAppMapGroup NetFlowCollector			
	EPP DstPort = 700 Def	faultAppMapGroup NetFlowCollector			
	ERPApplication DstPort >= 51000,DstPort <= Def	faultAppMapGroup NetFlowCollector			
	ESRO DstPort = 259 Def	faultAppMapGroup NetFlowCollector			
	Echo DstPort = 7 Def	faultAppMapGroup 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					
Configuration		Lea	f Collectors		
I eaf Collector Systems Ceaf Collectors Ceaf Remote Sources	Collector Name Status	IP NE TESE TESE TINK	Collector Type netflow	Collector System Hostna Listen Port nnmiwin66.ind.hp.com 9991	
Master Configuration #™Master Collector #™Master Remote Sources					

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

Save & Close Help		
Leaf Collector Details Instructions Collector Name NetFlowCollector Status RUNNING Collector Type netflow ▼ Listen Port 9991	Piled Filter Group Applied Application Mapping Groups TOS Groups Application Groups DefaultAppMagGroup Ø ImportantApplications	Flow Forwarding Destinations Flow Exporters Collect Number of Application Mappings 303 1
IP 145.1530.1556.1556		
Store Flow in File false -		
- DNS		
Source IP DNS Lookup false ▼ Destination IP DNS Lookup false ▼		

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

Traffic Reporting Nodes					
🗵 🖆 🧭 🖳 🌮 🔛				Ø	1-1 of 1
Three Node Name	Traffic Type	Tenant Name			
iscope6524	NetflowV9	Default Tenant			
Updated: 4/11/12 04:54:59 PM		Total: 1	Selected: 1	Filter: OFF	
Analysis					
Traffic Reporting Node Summary 😂		Top Apps-In 🕖 Top Apps-Out 🕄	Top ToS-In 😳 Top ToS-Out 🚭	Top IP Protocol-In 🍪	Top IP Protocol-O
Current Time Wed Apr 11 16:55 Analysis Period for Node Last 1 Hour Performance Data Wed Apr 11 16:55	:00 IST 2012 :00 IST 2012		ERPApplication(1627KBytes	5)	

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.

Metwork Node Manager iSPI Perfor	mance for Traffic	
Configuration		Type Of Service Groups
₩Leaf Collector Systems ₩Leaf Collectors ₩Leaf Remote Sources	TOS Group Name	Number of TOS Mappings
Master Configuration		
翻Master Collector 麵Master Remote Sources		
System Health		
ImInstallation Verification ImTraffic Health ImUnresolved NNM IPs		
Site, ToS and Threshold Configuration		
Type Of Service Groups		

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 TOS Operation TOS 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 16 false Collector File false Collec	Image: Point Poin
Start-Stop Time Sat, 14 Apr 2012 19:54:20 IST Last Stap Time Never Stopped Last Flush Time Sun, 15 Apr 2012 11:53:43 IST Number of Flushed 92 Number of Flushed 92	

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.

Network Node Manager iSPI Pe	rformance for Traffic			
Configuration		Sites	<u> </u>	
ELeaf Collector Systems	Site Name	Site Condition Site Description	Site Priority	Tenant
ImLeaf Collectors	🔲 Delhi	SrcIPILIKE! DstIPILIKE!1	1	Default Tenant
2001100000	Mumbai	SrcIPILIKE! DstIPILIKE!	20	Default Tenant
	Bangalore	SrcIPILIKE! IDstIPILIK	10	Default Tenant
Master Configuration	Hyderabad	SrcIPILIKE	7	Default Tenant
mMaster Collector	FortCollins	SrcIPILIKE!	9	Default Tenant
System Health				
Installation Verification				
#Traffic Health				
Contraction of the second seco				
Site, ToS and Threshold Configuration				
Sites				
Threshold				

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 space	es, no special characters except hyphen and underscore)
Site Description	,ivan,,
✓ 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 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.

Network Node Manager						User Name: system NNN	li Role: Adm
File View Tools Actions Help							
👌 Incident Management	* Traffic Sites						
🔥 Topology Maps	😺 🖉 🛛 🖻 🖉 🔍	🗟 🖗 🔛				K 🕥 1-	5 of 5
Monitoring	Site Name	Site Priority Site Description	Tenant Name				
Troubleshooting	* New York	10	Default Tenant				
Inventory		1	Default Tenant				
Management Mode	* Tokyo	9	Default Tenant				
🏷 Incident Browsing	Shanghai	7	Default Tenant				
🐺 Cisco IP Telephony	* Toronto	20	Default Tenant				
🖙 Nortel IP Telephony	*						
💱 Avaya IP Telephony	*						
🐼 Quality Assurance	*						
💱 Traffic Analysis	*						
Traffic Reporting Nodes Threshold Exceptions Reporting N Traffic Reporting Interfaces Threshold Exceptions Reporting In Threshold Exceptions Reporting In Traffic Stees	Updated: 4/17/12 04 Analysis Site Summary 🚱	:39:13 PM		Total: 5	Selected: 1	Filter: OFF Destination Site - Top Apps - In 🕲	Destinatio
< ,	Current Time Analysis Period for Site	Tue Apr 17 16:39:21		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.

🧑 Network Node Manager iSPI Perfo	rmance for Traffic			
Configuration Leaf Configuration Leaf Collector Systems Leaf Collectors Leaf Collectors Leaf Collectors Leaf Sempta Sources	Metric	Summary	Threshold High Value	High Rearm Value
Master Configuration ##Master Collector ##Master Remote Sources				
System Health ﷺInstallation Verification ﷺTraffic Health ﷺUnresolved NNM IPs				
Site, ToS and Threshold Configuration Sites Type Of Service Groups Threshold				

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

reshold Details				
Instructions				
etric Volume -	Application Mappings Sites			
gh Value GB •	Site Namp	Site Condition Site Description	Site Priority	Tenant
ch Rearm Value GB •	Delbi	SrcIP!LIKE St	1	Default Tenant
Application or ToS	Mumbai	SrcIPILIKE	20	Default Tenant
	Toronto	SrcIPILIKE	10	Default Tenant
Application	Mew York	SrcIPILIKETINA THAT * *	7	Default Tenant
All Applications	Tokyo	StcIPILIKE State Street	9	Default Tenant
Set Threshold By O ToS				
O All ToS				
None				
Topology Filters				
Interface				
Set Threshold By 💿 Node				
Site				
hese are just filters. Choosing Node/Site here does not imply Node/Site based incidents. All he Incidents are always at the Interface level.				
	-			

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

Save & Close Save & New Help				
Threshold Details				
Instructions				
Metric Bandwidth	Application Mappings Flow Enabled N	lodes		
High Value 200 Kbps -	Application Name	Condition Configuration	Application Groups	Collector Name
High Deser Volue 120	SIPoverTLS	DetPort = 5061	DefaultAnnManGroup	
High Ream value 150 https -	HPPataProtector	DstPort >= 2100 DstPort <=	ImportantApplications Defaul	NetFlowCollector
Application or ToS	PostOfficeProtocol3overTLSor	DstPort = 995	DefaultAppMapGroup	
Application	AccessNetwork	DstPort = 699	DefaultAppMapGroup	
All Applications	WHOISprotocol	DstPort = 43	DefaultAppMapGroup	
Set Threshold By ToS	TrivialFileTransferProtocol	DstPort = 69	DefaultAppMapGroup	
 All ToS 	NetIQEnd2End	DstPort = 2220	DefaultAppMapGroup	
None	Tripwire	DstPort = 1169	DefaultAppMapGroup	
	udt_os	DstPort = 3900	DefaultAppMapGroup	
Iopology Filters	ingreslock	DstPort = 1524	DefaultAppMapGroup	
Interface	NetIQMonitorConsole	DstPort = 2735	DefaultAppMapGroup	
Set Threshold By	KerberosversionIV	DstPort = 750	DefaultAppMapGroup	
Site	RemoteTELNETService	DstPort = 107	DefaultAppMapGroup	
These are just filters. Choosing Node/Site here does not imply Node/Site based incidents. All	dtspcd	DstPort = 6112	DefaultAppMapGroup	
the Incidents are always at the Interface level.	MITMLDevice	DstPort = 83	DefaultAppMapGroup	
	WAPpushMMS	DstPort = 2948	DefaultAppMapGroup	
	Symantecvnetd	DstPort = 13724	DefaultAppMapGroup	
	SAPro SAPro	DstPort >= 3000,DstPort <=	ImportantApplications, Defaul	NetFlowCollector
	NetBIOSSessionService	DstPort = 139	DefaultAppMapGroup	

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

4. 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 Sar	ve & New Help						
Threshold Details							
Instructions							
Metric	Volume -		Applic	ation Mappings Sites			
High Value	100	КВ 👻		Application Name	Condition Configuration	Application Groups	Collector Name
High Rearm Value	50	KB 👻		DanwareNetOpRemoteControl	DstPort = 1970	DefaultAppMapGroup	
- Application or ToS				DanwareNetOpSchool	DstPort = 1971	DefaultAppMapGroup	
				Discard	DstPort = 9	DefaultAppMapGroup	
	Application			DomainNameSystem	DstPort = 53	DefaultAppMapGroup	
	 All Applications 			DomainNameSystemRDNCS	DstPort = 953	DefaultAppMapGroup	
Set Threshold By	ToS			Doom	DstPort = 666	DefaultAppMapGroup	
	All ToS			EMCADS	DstPort = 3945	DefaultAppMapGroup	
	None			EMWIN	DstPort = 2211		
Tenelos, Eilten				EPP	DstPort = 700	DefaultAppMapGroup	
Topology Filters				ERPApplication	DstPort >= 51000,DstPort <=	stPort >= 51000,DstPort <= ImportantApplications, Defaul	
	Interface			ESRO	DstPort = 259	DefaultAppMapGroup	
Set Threshold By	Node			Echo	DstPort = 7	DefaultAppMapGroup	
	Site			FCIP	DstPort = 3225	DefaultAppMapGroup	-
These are just filters	. Choosing Node/Site here does no	t imply Node/Site based incidents. All		FTPControl	DstPort = 21	DefaultAppMapGroup	
the Incidents are alw	ays at the Interface level.			FTPControloverTLSorSSL	DstPort = 990	DefaultAppMapGroup	
				FTPData	DstPort = 20	DefaultAppMapGroup	
				FTPDataoverTLSorSSL	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.

Metwork Node Manager iSPI Perf	ormance for Traffic			
Configuration eaf Configuration	₱ ∆ ש₀		Threshold	
Leaf Collector Systems	Metric	Summary	High Value	High Rearm Value
Leaf Remote Sources	VOLUME	Sites: 1, Applications: 1	100.0 KB	50.0 KB
	BANDWIDTH	Flow Node: 1, Applications: 2	200.0 Kbps	130.0 Kbps
ster Configuration				
Master Collector				
Master Remote Sources				
vstem Health				
Installation Verification				
Traffic Health				
Unresolved NNM IPs				
te, ToS and Threshold Configuration				
Sites				
Threshold				

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	<u>}</u>	
2 🖻 🞜 🖪	🖗 🖼	
Thee Node Name	Traffic Type	Tenant Name
ciscope6524	Netflow//9 Select All Sort Filter Export To CSV Configure Traffic Threshold Traffic Maps Traffic Reports Quality Assurance HP NNM iSPI Performance	Default Tenant

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

Traffic Reporting Nodes T	raffic Reporting Node														
2 🖗 🖉 🔛															
✓ General			То	p 5 Sc	urces	s To	op 5 Des	tinatior	ns Top 5	Conversa	ations T	Traffic R	Reporting Interfaces	Applicable Threshold	Incidents
Node Name	ciscope6524	*	-												
Traffic Type	NetflowV9			2		0		P					🔯 🕥 1-	2 of 2	
Tenant Name	Default Tenant			Value	• •	Va	lue Unit		Rearm Va	alue	Rearm U	Jnit	Metric		
				100.0		к	в		50.0		КВ		Volume		
				200.0		к	bps		130.0		Kbps		Bandwidth		
				Upda	ed: 4/	17/12	2 04:57:2	6 PM			Total: 2	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.

I ratfic Reporting Nodes	s I ramic Reporting Node							
🖉 😼 😂 🔛	3							
			Top 5 Sources Top	5 Destinations Top 5 Conver	rsations Traf	fic Reporting Interface	s Applicable Threshok	d Incidents
Node Name	ciscope6524	*	-					
Traffic Type	NetflowV9		2 2 6	×		K 🕥 1	- 1 of 1	
Tenant Name	Default Tenant		Sever Lifecy Las	t Occurrence . Ti Corre Sou	Irce Node	Message		
			🙆 🖉. 4/43	/10.4/67/42 DM	0006524	One or more interface:	on node: cincone6524	ind he com has breached
			Updated: 4/17/12 0	4:57:53 PM	Total: 1	Selected: 1	Filter: OFF	Auto refresh: OFF
Analysis				_				
Incident Summary : No	odeTraffic 🚭	Details 😂	Custom Attributes	ciscope6524 MIB Values	Source No	ode ciscope6524 😂		
Performance Data	Tue Apr 17 16:58:03 IST 2012	Category	0	Performance				
Message	One or more interfaces on node: ciscope6524 has breached the traffic thresholds	Family Correlation Na	ature	Traffic Root Cause				
Severity	Critical	Last Occurre	nce Time	April 17, 2012 4:57	:43 PM			
Priority	com.hp.nms.incident.priority.High	Source Node		ciscope6524				
Lifecycle State	Registered	Source Object	t	ciscope6524				
RCA Active	false							
Source Object	ciscope6524 (Traffic Node Table Data)							
Created/Opened	4/17/12 04:57 PM (Open for 20.3 seconds)							

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

Traffic	Traffic Reporting Nodes											
2												
Three	Node Name	Traffic Type	Tenant Name									
	ciscope6524	NetflowV9	Default Tenant									
\smile												

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.

🕼 Network Node Manager									Role: A
File View Tools Actions Help									
👌 Incident Management 🛛 🕹 🕹	Threshold Exceptions Reporting In	terfaces							
🛧 Topology Maps 🛛 🕹	🗵 📓 🖉 🥫 🖗 I	×					ø	I-1 (of 1
Monitoring ×	These Interface Name	Hosted On	Traffic Type	Flow Process Te	nant Name				
Troubleshooting ¥	Gi1/1	ciscope6524	NetflowV9	✓ De	ault Tenant				
Inventory ¥	\bigcirc								
Management Mode *									
🇞 Incident Browsing 🛛 🗧 🕹									
💱 Cisco IP Telephony 🛛 🕹									
💱 Nortel IP Telephony 🛛 🗧 🛠									
💱 Avaya IP Telephony 🛛 🗧 🛠									
🛱 Quality Assurance 🛛 🕹									
Traffic Analysis *									
Traffic Reporting Nodes									
Threshold Exceptions Reporting Nor									
Traffic Reporting Interfaces			_						
Threshold Exceptions Reporting Inte	Updated: 4/17/12 04:59:23 PM		10	tal: 1	Selected, 1 Filter, OFF				
Traffic Sites	Analysis			7					
	Traffic Reporting Interface Summ	hary 😳	Top Apps-In 😂	Top Apps-Out 🕻	Top ToS-In 🕄	Top ToS-Out 💕	Top IP Protocol-In 🚭	Top IP Prot	tocol-O
	Current Time Tue Apr	17 16:59:26							
	Analysis Period Last 1 H	our							
	Performance Data Tue Api	17 16:59:26							
۰ III ۲			HPDataProte	ctor Undefined	ERPApplication	PriorityApp S	APro		
				_					

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.

1 Network Node Mana	ger									nstem 1000 Role: Administrator	Sign Out
File View Tools Actions I	Help										
Incident Management Open Key Incidents Unassigned Open Key Incidents My Open Incidents	¢ ents	Open Key Incidents	Last OccurrenceTi Assigned Ti Source 4117/12 4 57:43 PM ciscopel 4171/12 4 57:43 PM ciscopel 4171/12 4 57:43 PM ciscopel	Node Source Ob 1524 Gri/1 1524 Gri/1 1524 ciscope652	ect Ca	teç ramit (Traffe ¹ Traffe ¹	origii Ci	Last Week - <empty g<br="">orrer Message High traffic ingress volu High traffic ingress ban One or more interfaces</empty>	roup filter» - 6 me reported through an inter dwidth reported through an is on node: ciscope6524 has b	face Gil/1 on the node ciscope8524	Notes
		Updated: 4/17/12 05:0	0:23 PM		Total 3 Sel			Selected: 1 Filter: ON			Auto refresh: 30 sec
	_	Analysis									
.1. Topology Maps	¥	Incident Summary : I	nterfaceApplicationTraffic 🗯	Details	O Cu	stom Attribut	10	ciscope6524 MB Values 3	Source Node ciscope652	0	
Monitoring	¥	Performance Data	Tue Apr 17 17:00:30	Category				Performance			
Troubleshooting	¥		High traffic ingress bandwidth reported	d Family				Traffic			
Inventory	¥		ciscope6524 ind.hp.com for the applicat	tion Origin	on reature			NNMi			
Management Mode	×	Message	HPDataProtector Configured threshold Kbps and Measured value: 1092.3345947	1: 200.0 7265625 Last Oct	aurrence Ti	ne		April 17, 2012 4:57:4	3 PM		
🄥 Incident Browsing	¥		Kbps. Measurement time is: 2012-04-17	Source	iode			ciscope6524			
Staco IP Telephony	¥	Severity	16:57:41:118	Source	Direct			GILT			
Nortel IP Telephony	*	Priority	com.hp.nms.incident.priority.High								
🕎 Avaya IP Telephony	¥	Lifecycle State	Registered								
🕎 Quality Assurance	8	RCA Active	faise								
1 Traffic Analysis	*	Created/Opened	Gi1/1 (Traffic Interface Table Data) 4/17/12 04:58 PM (Open for 1.9 minutes)								

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.

(b) Network Node Manage	6												User Name: system NNM Role: Administrator	Sign Out	
File View Tools Actions Hel	9)														
ncident Management	*	Open	Key Inc	cidents											
Coen Key Incidents		19		0	8 🤊 🖗 🗱 🔛								Last Week + <empty filter="" group=""> = 10 0 1 - 10 of 42</empty>	3	
Unassigned Open Key Incidents		Seve	a Prior	ri Life	Last Occurrence-Ti Assig	ned Tr Source Node	Source Of	bject Ca	ites Fan		rigii	Cor	re Message	Not	
My Open incidents		0	s.	3	4/17/12 5:05:24 PM	ciscope6524	Gi1/1			14	3	1.4	High input utilization on interface Gr1/1 The inUtilizationState transitioned from NOMINAL to HK3H due to		
		0	2	3	4/17/12 4:57:43 PM	ciscope6524	Gi1/1		Trat	1/2	4	121	High traffic ingress volume reported through an interface Gif/1 on the node ciscope6524 ind hp.com in 1	c ,	
		0	21	5	4/17/12 4:57:43 PM	ciscope6524	ciscope652	24 6	Trat	fx 1	3	ų,	One or more interfaces on node: ciscope6524 ind hp.com has breached the traffic thresholds		
			5.0	3	4/17/12 4 24:17 PM	nnmiwin66.ind.hp	nnmiwin66	15	19 1	-	3	121	NNM health status is now at Warning		
		0	5.0	3	4/17/12 10:00:24 AM	ciscope6524	Gi1/3			-	3	1.	Interface Down		
		0	sI	8.	4/16/12 6 15 26 PM	ciscope6524	vrf-echo		Que	. 10		1.	The target address 172 16 113.9 is down.		
		0	5.0	3	4/15/12 3/22:01 PM	ciscope2051	ciscope218	51	Que		1	-	QA Probe ciscoce2051 ind ho com in the risk in TCP Connect failed to run. Reason: Oper state is No	10	
		0	5.0	8	415/12 5-52-27 AM	ciscone6524	ude	acho 4	0			1.1	QA Broke udgethe failed to put Beason Oner state is NetConnected		
		0	ell.		413/12 8 51 76 BU	circonality.	_ map		-		1		OA Bole Ins failed to use Basses One state is Noticesanded		
			-0		41312 0 31 28 PH	UBCOPEDD24				10			We neve		
		-		-	4/13/12 \$/41:17 AM	Ciscopeosz4	Gitti			- 24		-	interface pown		
		Updated: 4/17/12 05:06:31 PM				Total 42 Selected: 1 Filter: ON Auto refreat					h: 30 sec				
	-	Analysis										(
1. Topology Maps	×	Inck	dent Sur	mmary	InterfaceApplicationSiteTraffic	0	Detail	0 Cu	noten Att	Butes	0	ci	iscope6524 MB Values 🕼 Source Node ciscope6524 🕼		
Monitoring	¥	Pert	formanc	ce Data	Tue Apr 17 17:06:49 IST 2	012	Category Performance								
Troubleshooting	¥				high traffic ingress volu	reported through	Family						Traffic		
Inventory	¥				on interface Gi1/1 on the ciscope6524in DstSite	påde	Correla	tion Nature					Root Cause NNM April 17, 2012 4:57-43 PM ciscope0524		
Management Mode	¥	Mes	isage		for an application ERPAp	plication Configured	Last Oc	currence T	ine						
Incident Browsing	¥				811.6484375 KB. Measure	ment time is:	Source	Node							
Cisco IP Telephony	¥	2012-04-17 16:57:41:119			Source	Object					Gitt				
Nortel IP Telephony	×	Prio	et y		com ho oms incident or	iority High									
Avava IP Telephony	8	Life	cycle St	tate	Registered										
Quality Assurance	*	RCA	Active		faise										
Traffic Analysis	¥	Sou	rce Obj ated/Op	ject sened	Gi1/1 (Traffic Interface Tr 4/17/12 04:58 PM (Open fr	able Data) or 8.2 minutes)									

- 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.

Traffic Reporting Nodes					1-1 of 1	
Thee: Node Name	Traffic Type	Tenant Name				
ciscone6524	NetflowV9	Default Tenant				
Updated: 4/17/12 04:52:29 PM Analysis		Total: 1	Selected: 1	Filter: OFF		Auto refresh: 3 min
Traffic Reporting Node Summary 🚭		Top Apps-In 😗 Top Apps-Out 🕄	Top ToS-In 😂 Top ToS-Out 😭	🖇 Top IP Protocol-In 🚭	Top IP Protocol-Out 😏	Performance 3
Current Time Analysis Period for Node Performance Data Tue Apr 17 16:5:	2:34 IST 2012 2:34 IST 2012	CPU and Memory utilization biscop (CPU Utiliz	e6524 ×	Traffic flows - ciscope652 Number 0 2000 0 17.80 4/16/12	4 ind hp.com 23:00 05:00 1 4/16/12 4/17/12 4	X Volume - V Volume - Volume - Volume - Volume - Volume - Volume -

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.



Interface Interface Traffic 1 min - Headline Run Prompts Show Bookmark Help







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.

Traffic Reporting Nodes	s		
🗵 📑 💋 🖪	1		
Three Node Name		Traffic Type	Tenant Name
Cisco Select	ct All	low∨9	Default Tenant
Filter	ort To CSV	•	
Conf	figure Traffic Thresho	old	
Traff	fic Maps	•	
Traff	fic Reports	 Top Applications - Las 	ist Day
Qual	ity Assurance	Top Destinations - Las	ist Day
HP N	NM iSPI Performance	e 🔸 Top Sources - Last Da	Jay

• 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

Current Status		📇 Keep this version 🔻
User: tapan	MNM iSPI Performance	Interface Traffic 1 mins - Top N
Report: Top N Analysis Status: Ready Filter: Set	Run Prompts Help	
	Select Report Type	
Preferences	Top Interfaces	Check Topology Filter for set filters
Reports X Claco P Telephony Claco P Telephony SPI Metrics SPI Metrics SPI Metrics	Select Report Type	Confirm Selection
Schrittalin: Schriftalin: Schriftalin: Miterface_Traffic Miterface_Traffic_15_min Constraints_Traffic_1_min Miterface_Traffic_1_min Top N Analysis Top N Chart Analysis	Top Type of Service Top Destination Ports	

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

	Select Sources for P	pheanon		eep this version -
MNM	iSPI Performance		Interface Traffic 1 mins - Top N	
Run Prompts	Help			
Select Report Type				
	Top Applications	<u> </u>	Check Topology Filter for set filters	
Application Name	riorityApp		Confirm Selection	

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

Ø	NNM is	SPI Performar	nce	Interface Traffic 1 min - Sources_For_Applications - Top N			
<u>Options</u>	Run Prompts	Show Bookmark	Help				
🍸 Apr 17	7, 2012 9:55:00 PM -	Apr 17, 2012 10:55:00 F	PM (Last 1 Hour) (Server Time), Node Name	e ciscope6524 Application Name = PriorityApp, HPDataProtector			
Z Grouped by: Source Host Name							
™							
Rank	Source Host	Volume - In Bytes	Percent of ALL for Volume - In	Volume - Out Bytes Bar Chart for Volume - In Bytes			

Name (sum) Bytes (sum) (sum) (sum) 1 30,127,760 98,78% 0 2 211,872 0.69% 0 3 57,680 0.19% 0 4 25,668 0.08% 0 5 14,400 0.05% 0 6 9,680 0.03% 0 7 5,124 0.02% 0 8 5,040 0.02% 0 9 4,800 0.02% 0 10 4,800 0.02% 0 0/bers 31,784 0.10%	NULL	Source host	volume in bytes	Tercent of ALL for volume in v	olume our bytes	bar chart for volume	III Dytes
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		Name	(sum)	Bytes (sum)	(sum)		(sum)
$\begin{array}{c c c c c c c c c c c c c c c c c c c $	1	15.15536.36	30,127,760	98.78%	0		
3 57,680 0.19% 0 4 25,668 0.08% 0 5 14,400 0.05% 0 6 9,680 0.03% 0 7 5,124 0.02% 0 8 5,040 0.02% 0 9 4,800 0.02% 0 10 4,800 0.02% 0 0thers 31,784 0.10% 0	2	AN. 1285, 1286, 1125	211,872	0.69%	0		
4 25,668 0.08% 0 5 14,400 0.05% 0 6 9,680 0.03% 0 7 5,124 0.02% 0 8 5,040 0.02% 0 9 4,800 0.02% 0 10 4,800 0.02% 0 0thers 31,784 0.10%	3	17日、第二日年	57,680	0.19%	0		
5 14,400 0.05% 0 6 9,680 0.03% 0 7 5,124 0.02% 0 8 5,040 0.02% 0 9 4,800 0.02% 0 10 4,800 0.02% 0 0thers 31,784 0.10%	4	103, 103, 10305, 22	25,668	0.08%	0		
6 9,680 0.03% 0 7 5,124 0.02% 0 8 5,040 0.02% 0 9 4,800 0.02% 0 10 4,800 0.02% 0 0thers 31,784 0.10%	5	103 103 1030 2	14,400	0.05%	0		
7 5,124 0.02% 0 8 5,040 0.02% 0 9 4,800 0.02% 0 10 4,800 0.02% 0 0thers 31,784 0.10%	6	15.15536.80	9,680	0.03%	0		
8 5,040 0.02% 0 9 4,800 0.02% 0 10 4,800 0.02% 0 0thers 31,784 0.10%	7	话题而演	5,124	0.02%	0		
9 4,800 0.02% 0 10 4,800 0.02% 0 0thers 31,784 0.10%	8	话语而用来	5,040	0.02%	0		
10 4,800 0.02% 0 <u>Others</u> 31,784 0.10%	9	18.126 第.251	4,800	0.02%	0		
<u>Others</u> 31,784 0.10%	10	175.46.154	4,800	0.02%	0		
		<u>Others</u>	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.

MNM iSPI Performance

Interface Traffic 1 min - Sources_For_Applications - Top N

Options Run Prompts Show Bookmark Help

<u>~</u>___

🝸 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 Site Name : Destination Site Name

• ••							
Ranl	۰(Source Site Name	Destination Site 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		Atlanta	Tokyo	30,162,972	98.90%	0	
2		London	Bangalore	222,792	0.73%	0	l
3		Hong Kong	Mexico City	57,680	0.19%	0	l
4		Toronto	Atlanta	40,068	0.13%	0	I
5		Default	Tokyo	10,256	0.03%	0	l
6		Phoenix	Hong Kong	4,800	0.02%	0	l
7		Atlanta	Default	40	0.00%	0	l
	4	<u>Others</u>		0	0.00%		

Generated at : 11:01:43 PM (Server Time)

NNM iSPI Performance Interface Traffic 1 min - Sources__For__Applications - Top N Ø Hide Options Run Prompts Show Bookmark Help **Report Options** Top / Bottom 'N' Grouping by: Top 10 • Source Site Name • Destination Site Name - X ÷ Select Metric(s): Volume - In Bytes (sum) -7 Volume - Out Bytes (sum) - 7 ÷ Select a metric * Number of Flows - Incoming (sum) Number of Flows - Outgoing (sum) Confirm Selection Number of Packets - Incoming (sum) Number of Packets - Outgoing (sum) Period Length (secs) (sum) ne), Node Name = ciscope6524, Application Name = PriorityApp, HPDataProtector Volume - Out Bytes (sum) Sample Count (sum) Σ Interface ID (countDistinct) Interface Name (countDistinct) Qualified Interface Name (countDistinct) Node Name (countDistinct) Rc Interface ODBID (countDistinct) t of ALL for Volume Volume - Out Bar Chart for Volume - In Node ODBID (countDistinct) - In Bytes (sum) Bytes (sum) Bytes (sum) Interface UUID (countDistinct) 98.90% 0 Interface Alias (countDistinct) 0.73% 0 Interface Physical Address (countDistinct) Interface Type (countDistinct) 0.19% 0

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 thei SPI.

I	NNM iSPI	Performance	e	Interface	Traffic 15 min - Top	o_TypeOfService - Top N (Chai
Hid	e Options Run Prompts	Show Bookmark	<u>Help</u>				
R	eport Options						
	Top / Bottom 'N' Top 10			Grouping by:	_		
	Volume - In Bytes (sum)		• 7	Volume - Out Bytes (sum))	• 7	
Ð	Ĵ		_	•			
						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.

